NCS TIB 02-4

NATIONAL COMMUNICATIONS SYSTEM

TECHNICAL INFORMATION BULLETIN 02-4

Advancements in Photonic Network Architecture Migration:

The Evolution and Deployment of Multiprotocol Label Switching (MPLS), Generalized Multiprotocol Label Switching (GMPLS), and Advanced Optical Switching

May 2002

OFFICE OF THE MANAGER
NATIONAL COMMUNICATIONS SYSTEM
701 SOUTH COURT HOUSE ROAD
ARLINGTON, VA 22204-2198

This document was prepared under contract to the

Office of the Manager
National Communications System

Contract No. F41621-98-D-5625
Work Order No. 0022

Prepared by:

Gary L. Ragsdale, Ph.D. and Ryan D. Lamm
Southwest Research Institute™
P.O. Drawer 28510
San Antonio, TX 78228
210-522-3743 (VOICE)
210-522-5499 (FAX)

SwRI™ Project No. 10.04882

EXECUTIVE SUMMARY

Motivation for protocol developments like Multiprotocol Label Switching (MPLS) and Generalized Multiprotocol Label Switching (GMPLS) arise from fundamental shifts in the telecommunications market demand. Commercialization of the Internet, rapid moves to electronic commerce (e-commerce), and heavy investments in “dot-com” start-up ventures during the 1990s created a market in which data traffic doubled every six months.

The static nature of the current carrier network architecture left many carriers unprepared for provisioning large amounts of fiber and optical wavelengths to meet the needs of enterprise Internet Protocol (IP) networks, Internet Service Providers (ISPs), Virtual Private Networks (VPNs), and other data-centric services. The Synchronous Optical Network (SONET)-based control structure of carrier networks built during the last decade could not cope with the rapidly growing and changing service demands.

MPLS is a new branch on the data switching evolutionary tree derived from its ancestors: Consultative Committee on International Telegraphy and Telephony (CCITT) network protocol (X.25), frame relay, and Asynchronous Transfer Mode (ATM). MPLS addresses the growing popularity of TCP/IP transmissions. It assigns fixed length labels to packets for rapid and efficient packet relay between ingress and egress points near the network edge. Conventional IP forwarding routers deliver packets to end systems over access network technology (e.g., ATM, frame relay, Ethernet, X.25).

GMPLS, which is a superset protocol including Multiprotocol Lambda Switching (MPλS), was developed to support the benefits of MPLS over different types of transport networks such as spatial switching, optical wavelength switching, and time-division (SONET) multiplexing. GMPLS provides the control mechanisms required to bridge the gap between electronic and optical intelligent traffic forwarding methods. The authors of “Generalized Multiprotocol Label Switching: An Overview of Routing and Management Enhancements”[5] foresee the eventual consolidation of the four network layers into as few as two layers consisting of GMPLS and Dense Wavelength Division Multiplexing (DWDM). They foresee GMPLS bypassing the ATM and SONET layers. Advancements in optical switching technology bring the industry closer to all-optical processing, thereby greatly influencing future network design philosophies and fundamentals. Protocols like MPLS/GMPLS will aide in bridging the gap between electronic edge and all-optical network cores.

The expected migration to IP protocols including MPLS and GMPLS will be gradual. ATM and SONET equipment represent the preponderance of the electronic communications equipment within carrier networks.[38] Capital spending is largely curtailed to that of meeting network traffic demand for existing services. Carrier equipment may not recover to pre-2001 recession levels until mid-year 2003.

The International Telecommunications Union – Telecommunication - Standardization Sector (ITU-T) may or may not choose to sanction MPLS or GMPLS.[3] The ITU-T and American National Standards Institute (ANSI) are working together to create an overlay signaling protocol for optical networks using a client-based approach under the auspices of the Automatic Switched Transport Network (ASTN) and Automatic Switched Optical Network (ASON) standards.[47] It is considering several options under a concept called the "Architecture for Optical Transport Networks (AOTN), " ITU-T Standard G. 872. Ultimately, the ITU-T may choose an alternative approach and may ignore MPLS, GMPLS, or both. The lack of ITU-T involvement in MPLS and GMPLS may derail global adoption of these protocols.

TABLE OF CONTENTS

LIST OF FIGURES

LIST OF TABLES

LIST OF ACRONYMS

ADM	Add/Drop Multiplexers
ANSI	American National Standards Institute
ARIS	Aggregate Route-Based IP Switching
ASON	Automatic Switched Optical Network
AT&T	American Telephone and Telegraph
ATM	Asynchronous Transfer Mode
BGP	Border Gateway Protocol
BUS	Broadcast and Unknown Server
CATV	Cable Television
CCITT	Consultative Committee on International Telegraphy and Telephony
CLEC	Competitive Local Exchange Carrier
CLIP	Classical IP over ATM
CLNP	ConnectionLess Network Protocol
CoS	Class of Service
CPE	Customer Premises Equipment
CR-LDP	Label Distribution Protocol with Constraint-Based Routing
CSR	Cell Switch Router
DARPA	Defense Advanced Research Projects Agency
DIFF-SERV	Differentiated Services
DLCI	Data Link Connection Identifier
DOCSIS	Data Over Cable Service Interface Specifications
DS	Differentiated Service
DSCP	DIFF-SERV Codepoint
DS-3	Digital Signal 3 = 44.736 Mbps
DSL	Digital Subscriber Line
DWDM	Dense Wavelength Division Multiplexing
E-LSP	Experimental LSP
FEC	Forwarding Equivalence Class
FSC	Fiber Switch Capable
GMPLS	Generalized Multiprotocol Label Switching
HFC	Hybrid Fiber Coax
IBT	In-Band Terminator
IEEE	Institute of Electrical & Electronics Engineers
IETF	Internet Engineering Task Force
IFMP	Ipsilon Flow Management Protocol
IGP	Interior Gateway Protocol
ILEC	Incumbent Local Exchange Carrier
I-PNNI	Integrated PNNI
IP	Internet Protocol
IPoA	IP over ATM
IPsec	Internet Protocol Security
ISDN	Integrated Services Digital Network

IS-IS	Intermediate-System-to-Intermediate-System Protocol
ISP	Internet Service Provider
ITU-T	International Telecommunications Union – Telecommunication Standardization Sector
IXC	Interexchange Carrier
L2SC	Layer-2 Switch Capable
LAN	Local Area Network
LANE	LAN Emulation
LDP	Label Distribution Protocol
LEC	Local Exchange Carrier
LER	Label Edge Router
LES	LAN Emulation Server
L-LSP	Label inferred LSP
LIS	Logical IP Subnet
LSA	Link State Advertisements
LSC	Lambda Switch Capable
LSP	Label Switched Path
LSR	Label Switched Router
MAN	Metropolitan Area Network
MIB	Management Information Base
MPλS	Multiprotocol Lambda Switching
MPLS	Multiprotocol Label Switching
MPOA	Multi-protocol over ATM
MPC	MPOA Client
MPS	MPOA Server
NHRP	Next Hop Resolution Protocol
NNI	Network to Network Interface
OADM	Optical Add-Drop Multiplexer
OBS	Optical Burst Switching
OC-1	Optical Carrier 1
OC-3	Optical Carrier 3
OC-12	Optical Carrier 12
OC-48	Optical Carrier 48
OC-192	Optical Carrier 192
ODSI	Optical Domain Service Interconnect
OIF	Optical Internetworking Forum
OLS	Optical Label Switching
OPS	Optical Packet Switching
OSI	Open Systems Interconnection
OSPF	Open Shortest Path First
OTS	Optical Tag Switching
OXC	Optical Cross-connect
PABX	Private Automatic Branch Exchange
PAR	PNNI Augmented Routing
PDH	Plesiochronous Digital Hierarchy
PHB	Per-Hop Behavior

PNNI	Private Network-Network Interface
PSC	Packet Switch Capable
PVC	Permanent Virtual Circuit
QoS	Quality of Service
RBOC	Regional Bell Operating Company
RFC	Request For Comment
RFD	Reserve-a-Fixed-Duration
RFI	Request For Information
RIP	Routing Information Protocol
ROI	Return On Investment
RSVP	Resource Reservation Protocol
RSVP-TE	RSVP with Traffic Engineering Extensions
SDH	Synchronous Digital Hierarchy
SITA	Switching IP Through ATM
SLA	Service Level Agreement
SNA	Systems Network Architecture
SNMP	Simple Network Management Protocol
SONET	Synchronous Optical Network
SS7	Signaling System 7
SVC	Switched Virtual Circuit
T-1	T-carrier system T-1 = 1.544 Mbps
TAG	Tell-and-Go
TCP/IP	Transport Control Protocol/Internet Protocol
TDM	Time Division Multiplexed
TDMC	Time-Division Multiplexing Capable
TE	Traffic Engineering
TFTP	Trivial File Transfer Protocol
TTL	Time-To-Live
UNI	User-to-Network Interface
VC	Virtual Circuit
VoIP	Voice-over-IP
VP	Virtual Path
VPN	Virtual Private Network
WAN	Wide Area Network
WDM	Wavelength Division Multiplexing
X.25	CCITT network protocol

1.0 MOTIVATIONS FOR HIGH-SPEED ROUTING

Motivation for protocol developments like MPLS and GMPLS arose from fundamental shifts in telecommunications market demand. For example, SONET, Signaling System 7 (SS7), and digital telephone networks sprung up, increasing demand for telephone, cellular telephone, and fax services during the 1970s and 1980s. Frame relay and ATM developed from the need for more efficient ways to handle enterprise data network traffic and a need to consolidate voice and data traffic on to a common, core network.

During the 1980s, data networks played a minor role in the definition of network architectures. Enterprise networks consisted largely of proprietary protocols like IBM Systems Network Architecture (SNA). IP traffic was largely an academic phenomena limited to an obscure research and development network called the “Internet.” Events in the 1990s such as the development of browsers, web servers, HTML, and opening the Internet to commercial applications created another market shift so large that its ramifications are not completely felt nor understood.

The need for better support for IP-centric network services came to the forefront during the Internet traffic explosion of the 1990s. Prior to the Internet boom, carrier networks, residential services, and to a somewhat lesser degree, enterprise networks were voice-centric. Data traffic represented a small percentage, both in terms of volume of network services consumed and in terms of carrier network revenues.

Commercialization of the Internet, rapid moves to electronic commerce (e-commerce), and heavy investments in “dot.com” start-up ventures during the 1990s created a market in which data traffic doubled every six months. Geometric growth in Internet traffic quickly thrust IP-centric networks into center stage in terms of popularity and in terms of new service demands placed upon carriers.

Industry observers forecast that the number of Internet users will double to 600 million by 2010.[1] Such growth will place new demands on service providers for capacity and reliability.

It is apparent that the rapid adoption of IP-centric data services operating over carrier networks altered the face of the telecommunications marketplace forever. It created new services, an explosion of data services, the dilution of voice services, and new customer service requirements. The dominance of IP-centric data traffic upstaged voice networks and made voice-centric network architectures obsolete. The shift to IP-centric communication left large voids where users and telecommunications carriers, or simply “carriers”, alike found inadequacies in many established communication methods including SONET, frame relay, ATM, and hop-by-hop IP packet routing.

1.1 Suppliers See Opportunities to Sell New Network Equipment

Motivation for better IP packet forwarding methods comes from three primary camps: equipment manufacturers, corporations, and carriers. Equipment manufacturers hope to cash in on the Internet bonanza by selling new equipment that replaces the large base of existing IP routers, frame relay, ATM, and SONET equipment currently operating within the carrier networks.

Router manufacturers seek new packet forwarding technologies that scale to larger traffic volumes, primarily for their carrier customers. Enterprise, small business, and residential networks are "edge networks" that reside along the periphery of the carrier networks where IP traffic densities are low. Only large enterprise networks with extensive multimedia applications are likely to be near-term customers for a new generation of IP forwarding technologies like MPLS or GMPLS.

For the most part, enterprise networks subscribe to a carrier's high capacity core network for transport of traffic across a metropolitan area, within a country, and between countries. Traffic densities are low along the network edge. Conventional IP packet routing techniques are adequate, and even necessary, given the need for the application-specific services along the network edge. When edge network traffic reaches the carrier's network, many smaller traffic flows aggregate into heavy combined flows. The sheer volume of packet traffic within the carrier's core network quickly reaches levels that overwhelm conventional routing techniques.

Much of today's ISP and carrier network router equipment use the same hop-by-hop and deep packet header inspection routing techniques used in edge network routers. Routers using traditional IP routing techniques quickly reach capacity in the face of rapid IP traffic growth. Adding more routers increases operational complexity and cost much more rapidly than it adds new traffic forwarding capacity.

Many equipment manufacturers hope that MPLS, GMPLS, and advanced optical switching techniques will give them new packet forwarding technologies to offer to carriers. MPLS may offer advantages to some large enterprise networks. Most enterprise networks will continue to rely on Ethernet and conventional routing networks. Therefore, the near-term primary customer for MPLS, and virtually the only customer for GMPLS, is the carrier.

1.2 Enterprises Need Simplicity and Lower Cost

Enterprises need new services derived from new protocols like MPLS and GMPLS to simplify their operation and reduce communication service costs. Enterprises now operate sophisticated intranets for the purpose of managing their business, for advertising their products, and for conducting business with customers and suppliers. Enterprise networks span the globe, interconnecting corporate offices. Enterprises link together their many corporate intranets with point-to-point, VPN services.

Enterprise networks can be complex mesh networks consisting of many point-to-point private line or VPN connections. The many point-to-point connections required for a meshed network represent a significant portion of total business cost. Most corporations have difficulty justifying large investments in skilled staff to manage complex mesh networks. Consequently, corporations seek services that support their IP-centric enterprise networks and simultaneously reduce network management complexity and lower service cost.

Ideally, an enterprise needs a single VPN connection from each of its corporate intranets over which it would exchange traffic with every other corporate intranet location. The carrier's VPN service would distribute the corporation's packets according to information held in the packet header. Unfortunately, the ideal enterprise VPN service does not currently exist.

Today's implementations of frame relay and ATM-based VPN services do not adequately address enterprise network needs. Limitations in carrier billing, network management, and network equipment prevent carriers from providing fully routed, bandwidth-on-demand VPN services. Instead, carriers provide point-to-point intranet connections that emulate dedicated private line services between two intranet locations. All routing takes place within the enterprise's intranet routers. The number of VPN connections needed to maintain a meshed network between intranets grows geometrically as the number of intranets increase. Corporations find themselves faced with large investments in network edge routers, large service outlays for the many VPN connections, and the heavy burden of network staff needed to operate the many routers and VPN connections.

1.3 Carriers Need New Services, More Revenue, and Lower Cost

Carriers face the daunting problems of lowering service prices to maintain competitive advantage, reducing operating cost to maintain profitability, and achieving substantial revenues to ensure adequate return on investment (ROI). Construction of fiber optic cable routes at $30,000 per mile and implementation of carrier-class network equipment is a capital-intensive endeavor.[2] The only remedy when faced with heavy market competition and large capital expenditures is for the carriers to achieve high utilization on their systems. Carriers exploit subscriber traffic patterns to achieve high network utilization and adequate ROI.

There exists the need for better methods for provisioning carrier services. Carriers must be more efficient in the provisioning of services and the operation of network infrastructure as a means to create greater profits.[3] Carriers must find ways to reduce manual provisioning costs, delays, and complexity. They need protocols that automate the provisioning process and create avenues for new value-added services.

The shift from voice-centric to data-centric services is driving the change. Voice service provisioning is a largely static process. Trunks provisioned between carrier telephone switches or enterprise private automatic branch exchanges (PABXs) remain in place for extended periods of time. Telephone switches allocate the bandwidth and derive revenues from the shared use of statically provisioned, voice trunk circuits. The shift to data-centric services changes the provisioning and revenue-producing paradigm.

Most service subscribers need access bandwidths that satisfy peak bandwidth requirements during the busiest hours of a heavy business day. Off-busy hour traffic is substantially less than the peak bandwidth requirement. Consequently, normal business patterns leave subscriber access lines underutilized during much of the time.

Carriers understand that subscriber lines produce high traffic demands during brief periods of time. They use the statistical variation of subscriber traffic to concentrate traffic before it reaches the network core. Switching systems along the network edge aggregate traffic, producing heavy traffic flows that efficiently use core network cable routes, multiplexers, and switching systems.

Carriers take every opportunity to resell under-utilized bandwidth to as many subscribers as good traffic engineering practice and customer satisfaction will permit. Carriers "overbook" subscription bandwidth by selling subscriber access lines having total bandwidth that exceeds the capacities of their core networks by many times. For example, standard telephone engineering practice over-subscribes residential telephone services by a ratio of six residential subscriber lines to every trunk line. Over-subscription of PABX lines is somewhat less at a ratio of four PABX subscriber lines per trunk line.

Similar opportunities exist to over-subscribe bandwidth in data networks. Carriers aggregate traffic from frame relay, cable modems, and Digital Subscriber Line (DSL) subscriber lines onto high-speed core networks comprised of ATM switches and SONET multiplexers. The subscribed bandwidth along the network edge is much larger than the network core bandwidth. Only by over-subscription bandwidth can carriers achieve adequate returns on investments at prices that subscribers will accept.

1.4 Deficiencies in Carrier IP Transport

It is essential that packet data networks like the Internet scale up rapidly to meet the growing demand for multimedia traffic.[4] IP networks must scale upward in their ability to handle greater bandwidths, route larger numbers of packets, provision for a larger number of customers, and provide higher degrees of quality of service (QoS). To date, the methods for supporting IP over carrier networks do not scale well as the speeds and volumes of IP traffic grow.

The classical way of constructing an enterprise data network using carrier services was to interconnect corporate sites with carrier-provided, private line services. All switching and routing occurred within customer premises equipment (CPE) located at each site. The carrier derived fixed bandwidth services from fiber optic routes using SONET multiplexers and provided the private line services to enterprise customers for a fixed monthly fee. There was no opportunity for the carrier to resell bandwidth; there were no opportunities for the carrier to increase service revenues, thereby improving returns on the carrier's capital investment; and there were few opportunities to provide value-added services to the enterprise customer.

Enterprise data networks relied on meshed, private line connections between corporate offices. For example, airline reservation networks consisted entirely of private line services interconnecting airports, reservation offices, and ticketing facilities. Enterprise networks developed sophisticated applications operating over these meshed networks of private line carrier services.

Despite their prestigious place in the corporate world during the 1980s, data communications represented a small portion of the carrier's total revenues. Fixed price, dedicated private line services are not a highly profitable service. So long as voice was the dominant service, the fixed price nature of private line facilities did not significantly dilute revenues or profits.

The carrier business model depends upon a substantial amount of bandwidth resale revenues and shared use facilities like telephone trunks within a carrier's revenue mix. Carriers cannot make adequate profit margins from fixed private line facilities. Much of a carrier's revenue and profit depends upon the carrier's ability to resell bandwidth several times and manage the shared use of common facilities at high facility utilization. Otherwise, the capital investment associated with fixed revenue services, specifically private line services, becomes financially overwhelming.

An explosion of Internet traffic and broad shifts to data communications changed the subscription mix away from voice services in favor of data services. Rapidly growing and changing IP service demand pressured carriers to over-provision their networks, but to do so meant diminishing the carriers' profitability.

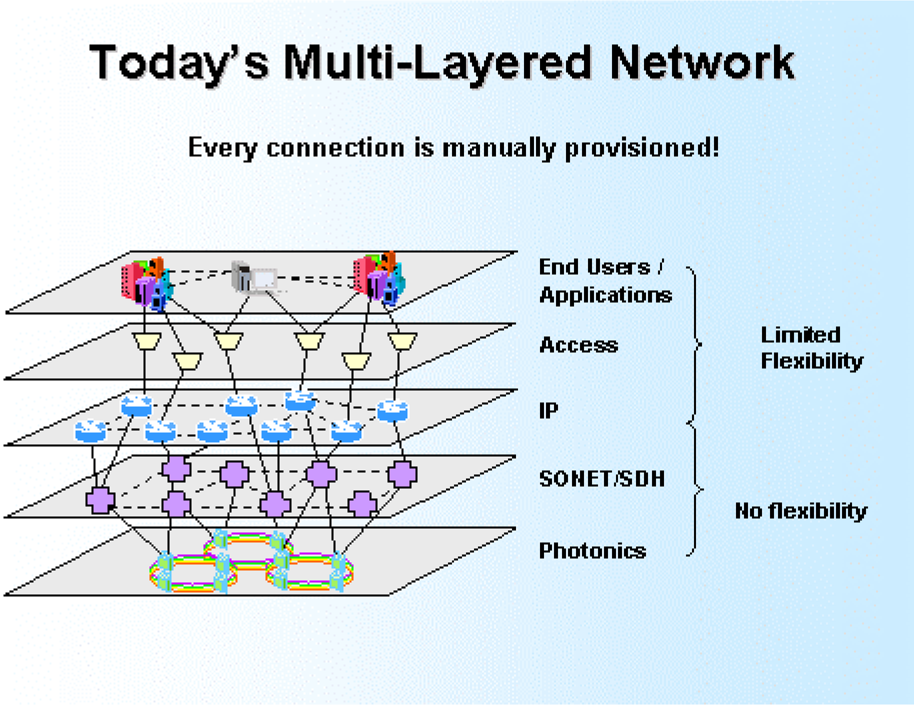
Unused bandwidth is a financial burden in a capital-intensive carrier network. The cost of fiber construction at $30,000/mile and carrier-class network equipment weighs heavily on the carrier's balance sheet. There is a need to rethink the carrier network architecture.

1.4.1 Outdated Network Architectures

Today's carrier-class data services network consists of five layers: a local access layer connecting enterprise networks to the carrier network, IP for carrying data applications, ATM for traffic engineering, SONET for transport, and wavelength division multiplexing (WDM) for capacity.[5] IP supports the wide variety of data and voice-over-IP (VoIP) applications dominating traffic growth in the networks. ATM supplies the QoS and service guarantees for reliability. ATM provides the means for engineering the flow of traffic. SONET networks are pervasive in their ability to distribute traffic reliably within the Metropolitan Area Network (MAN) and Wide Area Network (WAN). Carriers implemented WDM extensively to augment the capacity of their installed base of fiber.

Carriers manage each layer separately and use each layer to perform one function as well as possible. Each layer relies on a different control and data plane technology. Carriers create the network layers using fiber optic patch panels and switches for provisioning fiber optic links, WDMs for combining multiple optical paths onto a single fiber optic link, Optical Cross-connects (OXCs) for light path selecting optical paths within a fiber optic link, SONET for grooming optical channels (e.g., OC-3s, OC-12s,) onto light paths, and ATM switches or IP routers for consolidating customer traffic into optical channels. Each layer has its own network management system.

Figure 1 illustrates a typical layered network architecture without the use of ATM, i.e., the example shows an enterprise network using IP-over-SONET services. The IP layer gives the carrier some automation in traffic distribution and service provisioning. The SONET and WDM layers are static network layers that must be manually provisioned. The IP layer provides little in the way of traffic engineering control or QoS guarantees. Consequently, carriers must use manual provisioning to implement traffic engineering policies and to address performance deficiencies. Thus, the layered network design leads to frequent manual reconfigurations of the SONET and WDM layers for IP-related services.



© Scott Clavena, "Optical Signaling Systems," Light Reading, Inc., January 28, 2002
http://www.lightreading.com/document.asp?site=lightreading&doc_id=7098&page_number=1

Reprinted with Permission of Light Reading, Inc.

Figure 1: Layered Network Architecture [3]

This layered design works well when customer demand is relatively static, making provisioning costs a small part of total service costs. However, the annual doubling of Internet bandwidth demand driven by greater use of Internet services created a clamor for higher bandwidths, faster provisioning, more reliable services, and lower cost bandwidth. Internet traffic patterns are highly variable, unpredictable, and involve large bandwidths. The size and variability of the demand placed large, recurring provisioning burdens upon the carriers.

1.4.2 Deficiencies in IP over SONET

The cost and complexity of network provisioning became a significant impediment for carriers. New customer demand approached optical speeds of OC-48 and higher, thereby outstripping the economies of SONET time division multiplexed (TDMs). The layered network architecture could not scale fast enough and efficiently enough to satisfy customer demand and ensure carrier profitability. There was a growing need to simplify the control structure and consolidate network management within a single management paradigm.

The static nature of the current carrier network architecture left many carriers unprepared for provisioning large amounts of fiber and optical wavelengths to meet the needs of enterprise IP networks, ISPs, VPNs, and other data-centric services. Manual provisioning left the carriers with a complex collage of multiplexers, OXCs, and fiber patch panels. Customers wanted rapid provisioning and flexible deployment of services.

The SONET-based control structure of carrier networks built during the last decade could not cope with the rapidly growing and changing service demands.

The first portion of the system to become uneconomical under an onslaught of growing IP demand was the SONET add-drop multiplexer (ADM) rings. SONET rings failed to provide an economical means for supporting IP traffic because:

- SONET equipment costs became prohibitive for provisioning services greater than OC-12.
- SONET lacked the ability to support rapid or on-demand provisioning of new services.
- SONET lacked a coordinated signaling system for provisioning across networks comprised of SONET equipment made by competing manufacturers.
- SONET lacks a coordinated signaling system for provisioning across competing carrier domains.

OC-48 and OC-192 SONET ADM rings offer good economy for provisioning moderate speed services like 1.544 Mbps T-carrier system T-1 = 1.544 Mbps (T-1), Digital Signal 3 = 44.736 Mbps (DS-3), or OC-3 services. SONET multiplexers become uneconomical for provisioning OC-12 and higher speed services. Yet, many new service requests are for OC-12 and higher services to support growing IP traffic along the network edge. Carriers are replacing SONET with WDMs and OXCs as a means of providing better economy for wide bandwidth, OC-12 and higher speed services.

SONET multiplexer configuration systems rely on manual interaction and may control only a subset of a carrier's network. Provisioning services within or across carrier domains requires multiple, carefully coordinated interactions with several dissimilar SONET configuration systems. Carriers know how to manage and coordinate service provisioning across dissimilar systems. Even so, carriers are not equipped to handle rapidly changing service demands that require frequent reconfiguration of the SONET multiplexers. Growing demand to provision high bandwidth services, frequent provisioning of services to meet changing demand, and the complexity of the provisioning process left carriers with difficult network management problems and higher provisioning costs.

Carriers need new methods for provisioning optical bandwidths.[3] Carriers need a method for automatically provisioning shared-bandwidth across their networks. They need to support IP data traffic effectively, provide QoS guarantees for customer service level agreements (SLAs), and utilize core network bandwidth efficiently. Much of the current carrier network architecture lacks the ability to satisfy the needs of a growing variety of IP applications.

1.4.3 IP over Meshed Virtual Private Networks

The immediate solution to the carrier's private line profitability dilemma and growing IP services demand is VPNs. VPN is customer connectivity amongst several customer sites over a shared, usually public infrastructure employed with the same policies as a private network.[6] VPNs are one of the carrier industry's most successful services, having experienced double digit growth during the past several years.

As VPNs grew in popularity, there became an increasing need for more effective methods for provisioning and managing shared-use data communication networks. ATM and frame relay protocols provide infrastructure to support most VPN services, but they both lack scalable methods for handling large amounts of IP-centric data traffic. Moreover, the complexity of provisioning a large network of fully meshed ATM or frame relay permanent virtual circuits (PVCs) is complicated for the carrier and expensive for the enterprise customer.

1.4.4 Deficiencies of IP over Frame Relay Networks

Frame relay was the precursor to both ATM and MPLS. Frame relay developed as a direct result of modifications to the X.25 protocol. Its developers streamlined X.25 packet switching to achieve higher packet rates and wider subscription bandwidth. Frame relay was the first of the modern packet protocols to define the PVC concept for rapid relay of packets between two points at the edge of a network. The frame relay standard supports switched virtual circuit (SVC) connections for bandwidth-on-demand services, but carriers have not implemented frame relay SVC services, largely because the carriers lack methods to engineer and bill bandwidth-on-demand services.

Most frame relay VPNs follow the overlay model by providing point-to-point VPN connections. Provisioning frame relay VPNs use manual interactions with the frame relay network configuration system similar to those required for SONET private line provisioning. Frame relay customers typically pay a fixed monthly fee for each VPN PVC. Customers must manage routers capable of supporting the routing functions across multiple PVC alternatives. Consequently, carriers and frame relay customers suffer from many of the same provisioning and recurring cost problems that trouble SONET private line services, i.e., provisioning complexity and high recurring operational cost.

Carriers are considering MPLS in hopes of providing IP-centric VPNs at lower cost than VPNs provided by frame relay networks. For example, Cisco Systems claims that most of its 80 MPLS customers use MPLS to support VPNs.[1] MPLS could reduce VPN operation cost by as much as 50%. It is possible that MPLS savings and reduced provisioning complexity within the carrier's network will pass through as reduced complexity and savings for the enterprise. However, there are many outstanding implementation issues surrounding MPLS. Later sections of this report will discuss these issues and their possible ramifications.

1.4.5 Deficiencies of IP-over-ATM Networks

ATM overlays IP on top of its ATM signaling using protocols like Classical IP over ATM (CLIP), Local Area Network (LAN) Emulation (LANE), and Multiprotocol Over ATM (MPOA). These protocol overlays create Logical IP Subnets (LISs) within an ATM network. IP protocols operate in parallel with the ATM protocols without direct interaction like "two ships passing in the night." IP-over-ATM (IPoA) protocols create virtual connections (VCs) between LIS members. In most cases, IP routers are required to route packets between LISs.

All of the IP-over-ATM overlay techniques suffer from scaling issues.[4] Large numbers of VCs are necessary to create meshed network connections between LIS members. CLIP and LANE require IP routers to forward packets between LISs. Next Hop Resolution Protocol (NHRP) and MPOA attempt shortcut connections across LISs. However, both protocols suffer from traffic-driven routing delays, setup, teardown, and maintenance problems.

None of the IP-over-ATM protocols exploit the QoS features of ATM. Instead, the protocols emulate best-effort packet delivery common to conventional IP networks. IP-over-ATM overlay protocols waste investments in QoS mechanisms within an ATM network. Not even the most advanced IP-over-ATM protocol, MPOA, satisfies the need for IP transport over carrier core networks.

The ATM Forum created MPOA for the purpose of efficient transmission of unicast IP traffic between logical IP subnets in an ATM-based LANE environment.[7] It strives to use ATM SVC shortcut connections between edge devices, thereby bypassing intermediate routers.

MPOA consists of an MPOA server (MPS) and MPOA client (MPC). The MPS provides address resolution using the NHRP. The MPC identifies persistent data flows, and sets up and tears down shortcut connections between edge devices using the LANE protocol.

Standards development committees dropped several of the original requirements for MPOA. MPOA does not support multicast. There is no provision for firewall and layer 3-packet filtering functions. It does not support class of service distinctions, making QoS of IP traffic unavailable even though the capability exists within ATM. MPOA does not currently support VPNs. MPOA 1.1 Addendum adds VPN support, which corrects the lack of VPN support. A lack of interoperability between MPOA implementations is a lesser problem, but exists.

The MPOA standard leaves it to the implementer’s discretion to determine the persistence of a data flow. It suggests as a minimum that a threshold for the number of packets per second be used, but leaves the door open for implementers to use other criteria such as QoS. There are no specifics in the standard, and there are no hard requirements to support a specific MPOA VC shortcut algorithm.

MPOA has a number of serious deficiencies from the carrier viewpoint. The variety and number of shortcut connections established by MPOA make network problem analysis and traffic engineering difficult. MPOA is subject to single points of failure within LANE LECS, LES, and Broadcast and Unknown Server (BUS) devices. The ATM Forum released the LAN emulation network-network interface (LANE V2 LNNI) standard during 1999. The standard adds protocols for synchronizing redundant LANE servers and methods for achieving reliable LANE operation. Implementations of LANE V2 LNNI are rare.

Simple network management protocol (SNMP) is the protocol selected for management of MPOA devices. However, the ATM Forum and Internet Engineering Task Force (IETF) have been slow to define the SNMP Management Information Bases (MIBs) for MPOA. Consequently, there are difficulties in configuring MPOA devices from a central location. Consequently, network operators should only employ MPOA in small networks where the network management cost will be low. The limited MPOA management features leave carriers with a serious deficiency for the operation of their IP-centric services.

Multicast is a largely experimental and highly discussed concept for IP networks. Multicast is a difficult service to implement across an ATM network.[8] ATM connections are unidirectional by design. ATM supports point-to-multipoint connections. It does not support multipoint-to-point connections, often referred to as the "VC merge" limitation. ATM addresses multipoint-to-point traffic with multiple VCs, one for every pair of end points. The number of connections involved in large multicasts can starve the network of VCs and lead to scalability problems.

It appears that the leaders of ATM development expected ATM to replace Ethernet and IP to the desktop. The limited capabilities to support IP within Request for Comment (RFC) 1483, CLIP, LANE, and MPOA reflect a lack of support for IP-over-ATM on a large scale or within carrier networks.

The lack of network management, QoS, security, resilience, and multicast support makes MPOA a dubious choice for many situations. Its best application appears to be for small to moderate enterprise networks. It lacks many features essential to large corporate and carrier networks. MPOA is a useful extension to LANE in a LAN environment. It poses far too many problems for widespread use in a WAN.

The lack of adequate IP support within ATM led to the development of alternative protocols including MPLS and GMPLS as the demand for IP-based services outstripped all other services within communication networks.

In comparison, MPLS supports class of service and traffic engineering features. It supports multicast and VPN services. It is adaptable to ATM, SONET, and DWDM networks, while MPOA is an ATM-specific protocol.

2.0 THE EVOLUTION OF LABEL SWITCHING

Label switching is the evolutionary outcome of many prior standards and proprietary attempts at a better data switching protocol. The earliest days of label switching trace back to the ITU-T X.25 protocol. X.25 coined the term "virtual circuits" (VCs), commonly used in frame relay and ATM. It defined connection-oriented logical channel numbers with local significance. X.25 supports variable length packet transmission, as does frame relay.

Frame relay sprung up out of a need to streamline the X.25 protocol for operation at higher bandwidths over higher quality transmission systems, i.e., fiber transmission systems. Frame relay is also a connection-oriented protocol with virtual channels. The ITU-T ATM standard took X.25 and frame relay one step further and added many missing features like QoS and the ability to operate at speeds as high as 2.4 Gbps (OC-48).

Label switching is a new branch on the data switching evolutionary tree derived from its ancestors: X.25, frame relay, and ATM. It is an outgrowth of proprietary experiments to develop an IP-centric, connection-oriented protocol that addresses the growing popularity of TCP/IP transmissions.

Ipsilon IP switching, Toshiba's Cell Switch Router (CSR), Cisco System's Tag Switching, IBM's Aggregate Route-Based IP Switching (ARIS), and Telecom Finland's Switching IP Through ATM (SITA) are all proposed methods for creating more efficient core networks for IP traffic. All of the proposals use an exact match on a short, fixed length label. Hardware devices can more easily switch fixed length labels at higher speeds than the conventional IP address matching technique. These early label switching techniques are in general deficient in their ability to handle QoS guarantees, especially for the IP Switching, CSR, and Switching IP Through ATM techniques. The early techniques traverse ATM core networks but do not make use of ATM QoS guarantees.

2.1 Conventional IP Hop-By-Hop Routing

Today's IP routers use hop-by-hop routing with deep packet inspection to switch IP packets along connectionless routes. IP layer path reconfiguration is another way of saying "hop-by-hop IP packet forwarding." It offers fine grain routing of IP traffic at the price of high packet processing latency, jitter, and CPU-intensive route calculations.[9] IP packet forwarding is applicable in network edge devices, especially those located in enterprise networks. It is not scalable for use in large service provider networks where QoS guarantees and high bandwidth switching are prevalent.

2.2 Switching IP through ATM (SITA)

SITA is a Finnish Telecom proposal for connecting edge routers over an ATM core network.[10] The proposal performs VC merging by combining VCs at a router. VCs with a common destination are combined into a unique VPI, allowing merging of the flows without having to serialize cells within a packet. The limited number of VPIs within an ATM network limits the scalability of the SITA protocol.

2.3 Aggregate Route-Based IP Switching (ARIS)

The IBM-proposed ARIS encourages the development of ATM switches specifically designed to support VC-merging.[11] Packets arriving from different virtual path (VP)/VCs are merged and forwarded by retransmitting an entire datagram sequentially without cell interleaving. Alternatively, ARIS switches may merge VCs within a single VP. The later approach suffers from scalability problems tied to the relatively small number of VPs available within an ATM network. Routing is control driven using standard layer 3 protocols like Open Shortest Path First (OSPF) and Border Gateway Protocol (BGP). Egress routers define Label Switched Paths (LSPs) by sending ESTABLISH messages upstream toward potential ingress routers. Neighbors forward the ESTABLISH messages until they reach the edge of the ARIS control domain.

An important benefit of ARIS is its ability to prevent routing loops. ARIS guarantees that there will be no routing loops in any of its LSPs. Each router places its ID in the ESTABLISH message. It refuses ESTABLISH messages that contain its ID, thereby deleting loop routes as potential cut-through paths.

2.4 Cell Switched Router

Tokyo Institute of Technology proposed the CSR as an implementation of label switching.[12] Toshiba refined the proposal and promoted it as a product concept. CSR attempts to interconnect logical IP subnets within ATM VCs formed by running LANE or RFC 1577 Classical IP over ATM protocols. CSRs exchange signaling via the user-to-network interface (UNI) 3.1 Q.2931 protocol. Like the Ipsilon switch, CSRs will support both cell switching and IP forwarding. Unlike the Ipsilon switch, CSR will also support non-IP protocols.

2.5 Ipsilon IP Switch

Ipsilon Networks proposed its form of label switching created by combining an ATM switching fabric and an IP routing controller.[13] None of the ATM signaling or control plane appear within the IP Switch design. LSPs exist as PVC ATM connections. The IP controller establishes PVC paths via commands to the ATM switching fabric. During the early phases of flow transmission, Ipsilon switches forward packets using hop-by-hop IP forwarding. The switches assign labels to the packets and direct the traffic along LSPs when the switches detect long lasting flows. LSPs replace the conventional hop-by-hop IP forwarding process.

Ipsilon proposes Ipsilon Flow Management Protocol (IFMP) as the signaling protocol between routers in an MPLS network. IFMP does not create a most direct cut through path. Instead, the LSP follows the same hop-by-hop IP forwarding path. The ATM switching fabric in each Ipsilon switch bypasses the higher-level IP forwarding logic. However, the IFMP forwarding arrangement does not take advantage of ATM QoS guarantees.

2.6 Tag Switching

Tag switching is Cisco System's proposal for implementing label switching for IP networks.[14] The ingress router assigns a "tag," also referred to as a "label," based upon its destination IP address. Intermediate tag routers use the incoming tags to redirect the packet to an outgoing route. A new tag replaces the received tag at each router. Tag switching supports tag stacking to expedite packet switching at gateways between control domains.

Developers have difficulty mapping tag switching directly onto ATM. Tag switching proposals would replace the VPI/VCI field with the IP tag. On the surface, it would seem that the mapping should work well, but ATM does not support flow merging. There is no room within the VPI/VCI field for the time-to-live (TTL) field. Consequently, it is difficult to achieve the switching economies of stream merging. Since there is no way to determine how long the data has been circulating through the network, path loop detection is difficult.

Tag switching proposals espouse support for multicast. Publicity not withstanding, there is a lack of detail regarding how tag switching will implement multicast. Issues not withstanding, Cisco Systems' position as dominate router manufacturer will likely bring about similarities in the implementation of tag switching with that of MPLS.

2.7 The Vision for MPLS

It is essential that packet data networks like the Internet scale up rapidly to meet the growing demand for multimedia traffic.[4] They must scale upward in their ability to handle greater bandwidths, route larger numbers of transactions, provide for a larger number of customers, and provide greater Quality of Service within IP-centric networks.

MPLS replaces the standard destination-based hop-by-hop packet forwarding method employed within most IP networks with a label-swapping method similar to that employed by ATM and frame relay. It separates packet routing from packet forwarding, creating a "route occasionally, forward often" paradigm. MPLS can support protocols other than IP such as IPX and ConnectionLess Network Protocol (CLNP), but IP packet delivery is the primary motivator for MPLS development.

The designers of MPLS took advantage of existing ATM network topologies. In addition, they chose to use proven protocols like OSPF and BGP for routing. MPLS IP switching and ATM switching protocols can coexist on the same physical network, thereby creating several logical networks overlaid on the ATM network core.

MPLS is a standard set of protocols for the maintenance and distribution of labels with support for unicast, multicast, QoS, and explicit routing. Its design improves network layer scalability, supports traffic engineering along explicit routes, and provides greater price/performance for IP traffic traversing ATM or photonic networks.

3.0 MULTIPROTOCOL LABEL SWITCHING (MPLS)

Over the past several years, carrier networks have struggled to maintain adequate bandwidth to support the dramatic increase in Internet traffic. Demand for data has surpassed voice, introducing an entirely different set of network requirements. This increased demand and requirements shift, coupled with developments in digital video distribution, have caused transport engineers to evaluate new technologies to support this emerging multiprotocol environment. The goal is to provide a method of incorporating the requirements of voice, data, and video over a single network, to be able to delineate SLAs across this network to provide QoS, and to incorporate advancements in photonic network technologies to provide a scalable, fault-resistant, and efficient communication infrastructure.

Multiprotocol Label Switching (MPLS) evolved from protocols such as Epsilon’s "IP Switching," Cisco's "Tag Switching,” Toshiba's "Cell Switched Router," and IBM's ARIS. A working group within the IETF was created in 1997 to formalize these early developments into what is now called “MPLS.” [15][6]

MPLS (RFC 3031) can be viewed as an intermediary protocol, relating the Data Link Layer (Open Systems Interconnection [OSI] Layer 2) and the Network Layer (OSI Layer 3) to provide a means of controlling the way in which data flows across a complex multiprotocol network. MPLS uses the concept of Forwarding Equivalence Classes (FECs) to combine traffic of like type and/or destination and identify these aggregate flows with labels. MPLS provides QoS, support for VPNs, and traffic engineering.

3.1 Label Encoding

The MPLS protocol provides a relation between OSI Layer 2 and OSI Layer 3 traffic. In order to provide high-speed routing through the network, MPLS uses a label to distinguish different traffic classes or destinations. The label encoding method for packet based networks attaches a shim label between the Layer 2 data and Layer 3 header. This shim label is thirty-two bits (four octets) long and is segmented into four parts. Figure 2 graphically depicts the MPLS shim label inside a packet. The first twenty bits contain the MPLS label, which is an unsigned integer valued from decimal 0 through 1048575 that distinguishes the specific traffic route. The next three bits are deemed experimental and are used primarily to provide a means to determine a class of service (CoS) to relay information to the network routers about how to handle the traffic. The next bit provides a hierarchical label stack function. Finally, the last eight bits represent a conventional TTL, which provide network elements the ability to disregard a packet after a certain length of time to prevent endless recirculation loops through the network.[16][17]

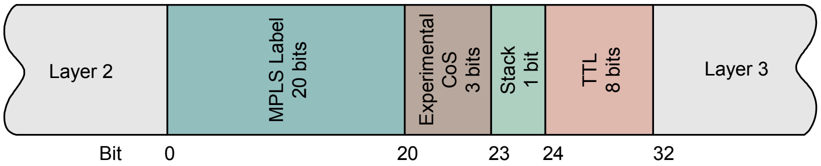


Figure 2: MPLS Shim Label

Another label encoding method involves native layer 2 encoding. This method is used for layer 2 technologies and involves embedding the twenty-bit label inside the link layer information. The label is embedded in the virtual path identifier/virtual channel identifier (VPI/VCI) for ATM and in the data link connection identifier (DLCI) for Frame Relay networks.[18] Figure 3 depicts the MPLS native layer 2 encoding for ATM.

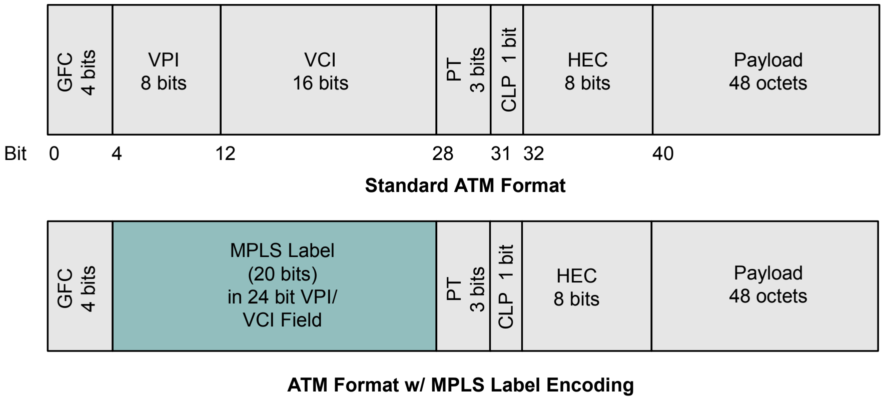


Figure 3: MPLS Native Layer 2 Encoding (ATM)

3.2 Method of Operation

Like ATM, MPLS is acronym intensive. The following is a list of commonly used acronyms that represent the components of an MPLS network.

- **FEC (Forwarding Equivalence Class):** A class or group of traffic based on common parameters, such as class of service. Defines a common set of packet handling parameters.
- **LSP (Label Switched Path):** A determined traffic path, through the MPLS network, from ingress to egress, with the same FEC and intended destination.
- **LER (Label Edge Router):** Routers that are MPLS aware, are located at the ingress/egress of the MPLS network, and perform the following functions:
    - Calculate the LSP through the MPLS network
    - Determine an appropriate FEC

  - Append the MPLS label at ingress of MPLS network
  - Remove MPLS label at egress of MPLS network
- **LSR (Label Switched Router):** Intermediate routers located along the LSP, on the inside of the MPLS network. LSRs inspect the MPLS label and forward traffic accordingly.

When the Label Edge Routers (LERs) receive a standard packet containing information destined to traverse the MPLS network, they attach the MPLS label. MPLS aware LSRs provide the high-speed traffic routing by only inspecting the MPLS label. The MPLS label directs traffic to specific predetermined LSPs, which are FEC based, aggregate multipoint-to-point traffic paths through the MPLS network. Further Layer 3 packet inspection is not performed until the packet exits the MPLS network through the egress LER. Once the egress LER receives the packet, the MPLS label is removed and the traffic is routed through the non-MPLS destination network without the MPLS label. Figure 4 depicts IP traffic traversing an MPLS network.

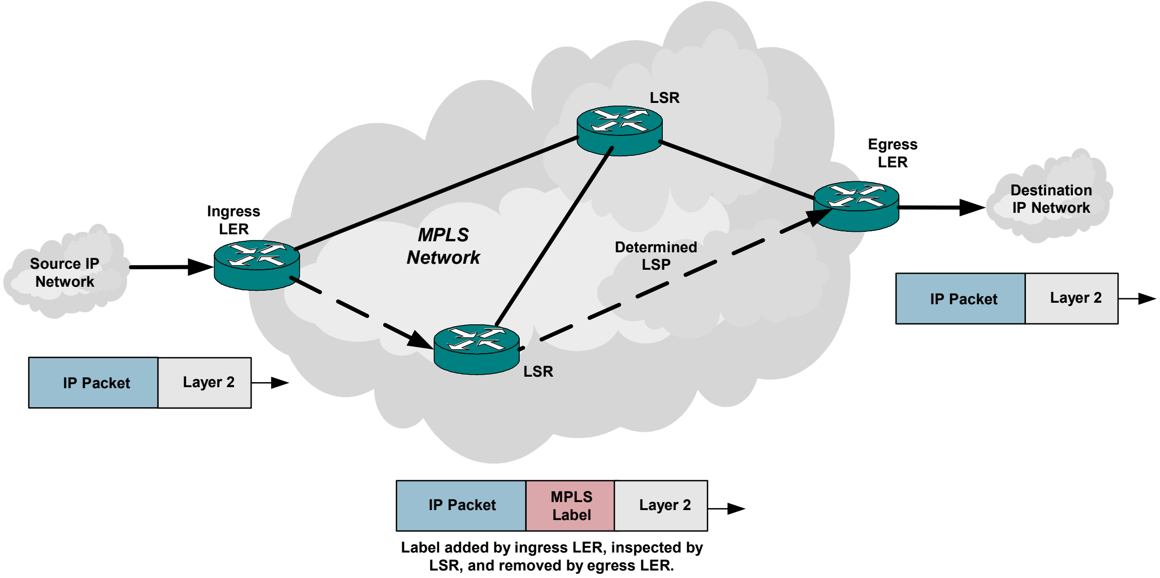


Figure 4: MPLS Network

3.3 Control Signaling

In order to reserve resources and manage LSPs over the MPLS network, it is necessary for the network to have some means of control plane signaling between LERs and LSRs. Two ways have been investigated to provide this signaling. Resource reservation protocol with traffic engineering extensions (RSVP-TE) and label distribution protocol with constraint-based routing (CR-LDP) both provide resource reservation, label distribution, LSP termination, and traffic engineering. Informational RFC 3210, issued December 2001, states: "CR-LDP and RSVP-TE are two signaling protocols that perform similar functions in MPLS networks. There is currently no consensus on which protocol is technically superior. Therefore, network administrators should make a choice between the two based upon their needs and particular situation."[19] The main difference between the two is the direction in which the resources are reserved during the signaling process and the transport protocol used. The following sections outline these MPLS signaling protocols. An extensive comparison between RSVP-TE and CR-LDP can be found in [20].

3.3.1 RSVP-TE

RSVP-TE operates by reserving resources in the reverse direction along the LSP and uses raw IP as its transport protocol. Figure 5 depicts the RSVP-TE downstream-on-demand signaling process. First, (1) the source sends a RSVP-TE "path message" to the receiver to establish the connection. (2) When the ingress LER receives the "path message," it injects a "Label_Request object" into the "path message" to request a label binding. The modified "path message" is then forwarded on to the adjacent LSR. The forwarding continues until the "path message" is received by the egress LER. (3) When the egress LER receives the "path message," it generates a "Resv message" which includes a "Label object." The egress LER then propagates the "Resv message" back to the adjacent LSRs. (4) When the adjacent LSRs receive the "Resv message," they will reserve the necessary resources, enter the new LSP label into their forwarding table, and forward the "Resv message" onto the next adjacent LSR, back towards the source. (5) If, however, a LSR does not accept the "Resv message," for reasons such as resources unavailable, the LSR will respond to the egress LER with a request to terminate signaling. (6) Once the ingress LER receives the "Resv message," it will append the LSP MPLS label to the data packets and forward the traffic through the network along the predetermined, resource reserved, LSP. (7) Each intermediate LSR along the LSP will inspect only the label, compare it to its forwarding table, and deliver the packet to the next LSR in the LSP. (8) When the egress LER receives the MPLS packets it will remove the label and deliver the packets to the destination.[21] Notice the end-to-end link evaluation prior to resource reservation.

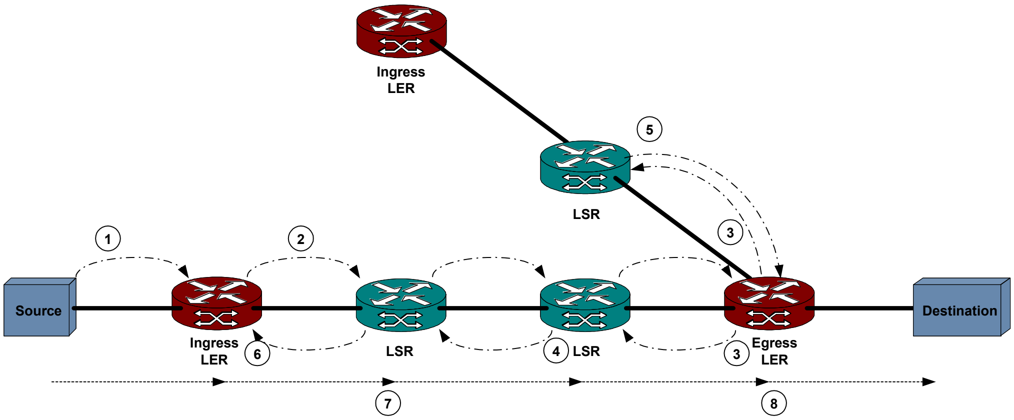


Figure 5: RSVP-TE MPLS Signaling

3.3.2 CR-LDP

CR-LDP operates by reserving resources in the forward direction and uses TCP as its transport protocol. Resources are reserved along each segment of the network in turn. Several methods of label distribution can be implemented with CR-LDP. Downstream-unsolicited and hop-by-hop/explicit route downstream-on-demand label distribution can be implemented. Figure 6 depicts downstream-unsolicited label distribution utilizing CR-LDP MPLS signaling, and Figure 7 depicts downstream-on-demand label distribution.

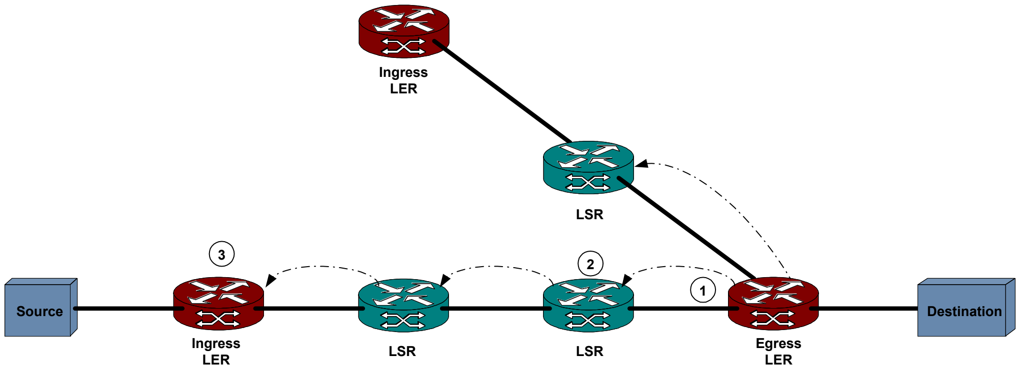


Figure 6: CR-LDP Downstream-Unsolicited Label Distribution MPLS Signaling

Downstream-unsolicited label distribution is accomplished when the egress router advertises without a label request. First, (1) the egress LER sends out a label mapping message advertisement to its adjacent LSRs. (2) The adjacent LSR then reserves the resources for that egress LER and forwards it on to its adjacent LSRs. (3) Once the ingress LER receives this message the LSP is established.

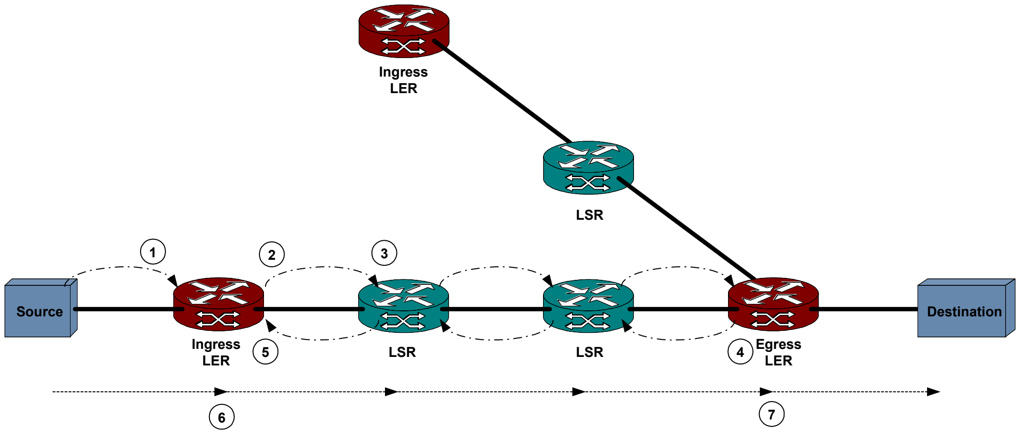


Figure 7: CR-LDP Downstream-on-Demand Label Distribution MPLS Signaling

Downstream-on-demand label distribution can occur by either hop-by-hop or explicit routing. Explicit routing involves the pre-establishment of an intended LSP path prior to signaling. Hop-by-hop CR-LDP downstream-on-demand label distribution operates by reserving the resources in the forward direction one segment at a time towards the destination. First, (1) the source will attempt to send traffic to the destination through the ingress LER. (2) The ingress LER will generate a Label_Request_Message and distribute it to the adjacent LSRs. (3) If an adjacent LSR accepts the Label_Request_Message and can allocate the requested resources, it will do so and forward the Label_Request_Message to its adjacent LSR in the direction of the destination. (4) Once the Label_Request_Message is accepted by the egress LER, it will generate a Label_Mapping_Message and forward it back to the LSRs toward the source.

When the LSRs receive the Label_Mapping_Message, they will compare the Label ID located in both the Label_Request_Message and the Label_Mapping_Message, and if it matches, the LSRs will add the label to their forwarding table and forward the Label_Mapping_Message to the next adjacent LSR in the direction of the source. (5) When the ingress LER receives the Label_Mapping_Message, it will perform the Label ID comparison and add the label to its forwarding table as well. (6) Finally, the label is attached to the packets and the traffic is forwarded through the MPLS network along the predefined LSP, without deep packet inspection. (7) When the traffic reaches the egress LER, the label is removed and the traffic is delivered to the destination.[20][21]

Both RSVP-TE and CR-LDP signaling protocols operate in conjunction with dynamic link state constraint-based routing protocols such as Intermediate System-to-Intermediate System protocol (IS-IS) and OSPF. These routing protocols are responsible for broadcasting status information, such as link constraint information, to all other routers in the network. This information is used to provide a means of QoS for the link.

3.4 Quality of Service

As networks converge and multi-service environments begin funneling diverse traffic across common transport protocols, a means of assuring quality levels for each data stream becomes critical. The bandwidth, latency, and jitter tolerances are different for voice, video, and data traffic, and the transport network must be able to provide quality levels for this myriad of traffic. MPLS provides QoS with two features: Class of Service (CoS) and Traffic Engineering (TE).

3.4.1 Class of Service (CoS)

CoS can be described as a course implementation of QoS that groups data flows based on similar types or classes and treats these classes according to similar performance criteria. CoS does not allow for the guarantee of bandwidth or the assurance of delivery time; however, it is more scalable than other QoS implementations. Differentiated Services (DIFF-SERV) is the CoS implementation that is being investigated for MPLS CoS.

DIFF-SERV groups data flows by associating Per Hop Behaviors (PHBs) with each flow. Per Hop Behaviors are different forms of treatments for packet forwarding. For this purpose, an IP header field, the Differentiated Service (DS) field, contains a DIFF-SERV Codepoint (DSCP), which relates the traffic to its representative Per Hop Behavior. Data flows are aggregated by their respective Per Hop Behaviors at the network edge devices, which then implement traffic policing to provide CoS to these aggregate flows. Moving the CoS processing to the edge network devices saves processing time in the core network elements, relieving them of CoS processing and freeing their resources for high capacity intra-network routing. It also allows the network to be more scalable to large networks while still providing end-to-end CoS.[22] There are two different methods for mapping DIFF-SERV to MPLS: Label inferred LSP (L-LSP) and Experimental LSP (E-LSP).

L-LSPs correlate the DSCP with the MPLS label. When the DSCP portion of the IP header is examined by the ingress LER, the LSP is assigned based upon the DSCP's Per Hop Behavior. The CoS is interpreted by the LSRs and the reservations are made accordingly. The egress LER will remove the label and the packet will be forwarded through the destination network based upon its original DSCP. The association of the DSCP and the MPLS label is critical and must be established before the data is transmitted. The second method for mapping DIFF-SERV to MPLS is E-LSPs. E-LSPs map up to eight DSCPs into the three bit experimental CoS portion of the MPLS label as seen in Figure 8.[23] LSRs handle E-LSPs in the same way they handle L-LSPs.

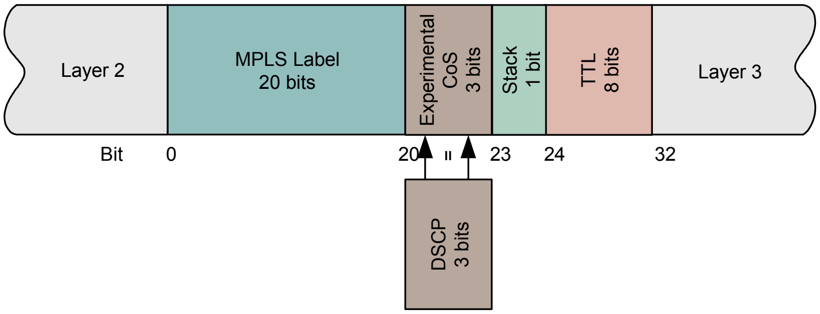


Figure 8: MPLS CoS E-LSP

3.4.2 Traffic Engineering (TE)

Traffic engineering provides the network the ability to intelligently handle administrative traffic decisions to increase network performance. These decisions are directly related to the utilization of bandwidth across the network and are essential for the networks to provide QoS. MPLS traffic engineering deals with:

- Establishment of LSPs
- CoS based LSP aggregation across the MPLS network
- Ability of an LSP to reroute
- Ability of an LSP to prioritize bandwidth reservation
- Distribution of traffic loads across parallel LSPs
- Ability for traffic to be superseded by higher priority traffic
- LSP's responsiveness to link failures and establishment requests [23]

Traffic engineering dramatically improves the resource management of the network. Without traffic engineering, it is difficult to ensure true QoS.

Traffic engineering relies on the ability to explicitly route traffic along designated routes. Traditional IP packet forwarding does not support explicit routing, thereby making traffic engineering difficult.[1] MPLS supports explicit routing and streamlines packet forwarding without deep packet inspection.

MPLS label swapping techniques are quite different from the packet inspection techniques of interior gateway protocols (IGPs) like Routing Information Protocol (RIP), BGP, and OSPF. All of the IGPs forward traffic along a route defined by the destination IP. The IGPs will continue to forward traffic along the route even if it becomes congested. Traffic engineers hope to use MPLS for more efficient use of all available links, reduce network latency, and provide QoS guarantees. Carriers hope to use MPLS traffic engineering to simplify IP network management.

Modern networks are dynamic systems that change through time. Consequently, MPLS networks use dynamic signaling and label distribution to accommodate changing network conditions.

MPLS supports dynamic signaling and label distribution in two forms: independent control mode and ordered control mode.[24] Independent control mode requires every router to listen to routing protocols, and construct its routing tables and distribute them independent of all other routers. Ordered control mode assigns the responsibility of routing table organization and distribution to one router, usually the egress router.

Each control method has its tradeoffs. Independent control achieves fast routing convergence. The lack of a central routing control point makes traffic engineering more difficult. Ordered control provides better traffic engineering control; however, it is slower to reach convergence and is vulnerable to single points of failure.

MPLS label distribution protocol (LDP) provides implicit routing. LDP uses a combination of the LDP for distributing the routing tables and BGP, and IS-IS for computing the contents of the tables' work in unison to define label LSPs within the network. They do not prevent traffic from merging onto congested LSPs. The implicit routing of the LDP and the lack of control over congestion can create serious problems for carriers as they try to engineer traffic flows and allocate finite bandwidth capacity within their networks.

3.4.3 Label Stacking

Desire to maintain SLAs between two networks that are disjoint across a third network results in the implementation of label stacking. Label stacking is a hierarchy-based implementation of MPLS that helps to provide QoS across multiple diverse third party networks, such as an ISP backbone. Additional MPLS labels are pushed onto the protocol stack as the packet enters the intermediate network and are popped off at the egress of the intermediate network. The traffic across the intermediate network is classified as tunneled traffic. Label stacking provides a means for best-effort traffic to be marked, classified, and policed to achieve end-to-end QoS.[17] Figure 9 depicts MPLS label stacking network topology.

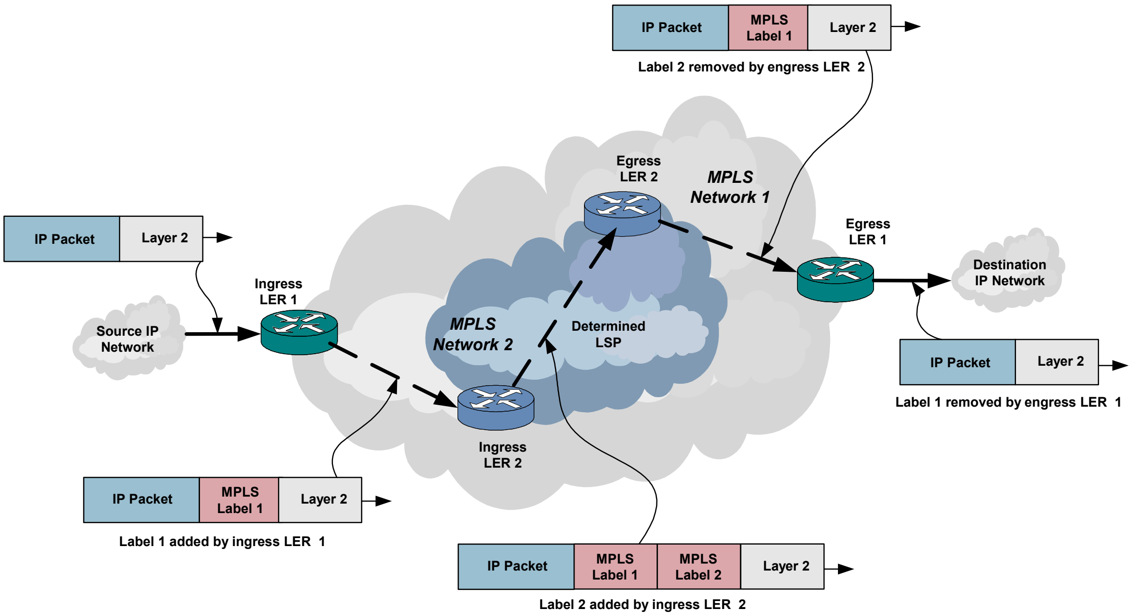


Figure 9: MPLS Label Stacking

3.4.4 Restoration and Reliability

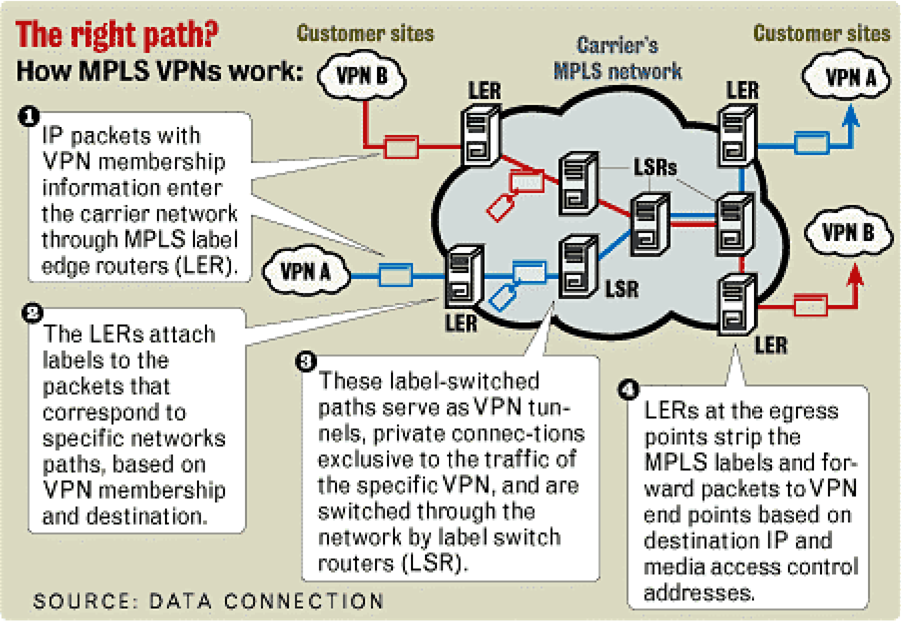
MPLS techniques can be implemented not only as a high-speed routing scheme for the electronic domain, but also can be applied in a modified form to the optical domain. Network restoration and reliability will be discussed further in terms of optical networks later in this report. For now, network restoration in the electronic domain via MPLS can be achieved via three different methods. The first and lowest level is link restoration, which involves the restoration of an LSP segment between two adjacent LSRs. This is a fast recovery technique; however, re-optimization of the network may be necessary from a traffic engineering perspective. The second restoration type is partial path restoration. Partial path restoration occurs around the down LSP segment. The LSR closest to the link failure on the ingress side reroutes the LSP around the failed link, to the egress LER. Finally, end-to-end restoration occurs when the entire LSP is renegotiated between the ingress LER and the egress LER.[21]

3.4.5 VPN Support

A dedicated transmission medium provides one of the most secure communication channels. Because installing dedicated physical media for every desired connection is both cost and spatially prohibitive, most corporations depend on public carriers/ISPs to provide a means of interconnecting offices, etc. VPNs have traditionally been implemented to protect sensitive data for transport over these public networks. A traditional IP VPN functions by establishing a tunnel from one network to another by means of encryption, such as Internet Protocol Security (Ipsec). Encryption codes are only known by the source and destination; therefore, sensitive traffic that is received by other destinations cannot be read and will be subsequently discarded. Use of encryption ensures data security in this connection-less environment by restricting the readability of the data.

For connection-oriented networks, such as Frame Relay and ATM, the data is not encrypted; however, the traffic is segregated by virtual-circuit. By completely isolating traffic streams, connection-oriented networks secure their data by preventing the data from reaching alternate undesirable destinations. Compromise of this security could be accomplished by misdirecting the establishment of the virtual-circuit, either by accident or intention.

VPN connections are supported by MPLS in two models. There is much controversy as to the true security of MPLS VPNs and their impact on the scalability and manageability of the MPLS network in general. MPLS VPNs for OSI Layer 2, called the overlay model, and for OSI Layer 3, called the peer model, have been proposed. RFC 2547 defines the peer approach, which uses BGP for signaling. The current debate about MPLS VPNs is not just which version to implement, but whether MPLS VPNs are secure enough that carriers will trust them for implementation. The lack of encryption of both the overlay model and peer model MPLS VPN connections is the main contention point. Figure 10 illustrates how the carriers might implement an MPLS-based VPN. Customer IP-over-frame relay or IP-over-ATM traffic arrives at an MPLS label edge router where it is adapted to the MPLS protocol. Label switch routers forward the MPLS packets through the network to a destination label edge router, where the customer traffic is converted back into conventional IP packets.



① IP packets with VPN membership information enter the carrier network through MPLS label edge routers (LER).

② The LERs attach labels to the packets that correspond to specific networks paths, based on VPN membership and destination.

③ These label-switched paths serve as VPN tunnels, private connections exclusive to the traffic of the specific VPN, and are switched through the network by label switch routers (LSR).

④ LERs at the egress points strip the MPLS labels and forward packets to VPN end points based on destination IP and media access control addresses.

SOURCE: DATA CONNECTION

Reprinted with permission of Network World

Figure 10: MPLS VPN Architecture [25]

In the overlay model, the carrier provides virtual connections between customer sites, but does not provide switching. Customer routers operating at the IP layer perform all routing between customer sites. Carriers only provide virtual private lines between the routers. For optimal routing, there needs to be a fully meshed set of connections between customer sites roughly equal to the square of the number of sites; i.e., the number of connections grows geometrically with the number of sites. The geometric relationship between the number of customer sites and the number of VPN connections creates scalability problems within the carrier network and within the customer routers. It adds complexity for the customer, because the customer's staff must maintain a complex network of routers and VPN connections.

The VPN peer model, on the other hand, requires that the customer router communicate with carrier switching systems. The customer router relays any packets with IP addresses not resident to the local domain to the carrier network. Carrier routers relay the packet over switched or routed paths to its destination at a remote customer site. To date, the peer model is not popular within carrier VPNs largely due to the major changes brought about by the peer model to carrier business practices. Carriers resist disclosing their network topology and resource information to customer routers. A portion of a carrier's network security strategy relies on obscuring the topology and resources within the network. Disclosing their network information may place the carrier at a competitive disadvantage with other carriers. Carriers provision VPN services using the same manually intensive methods found in most SONET networks. Consequently, the burden of VPN provisioning has become a serious concern. The pros and cons of each VPN implementation model are summarized in Table 1.

	Pros:	**Cons:**
Overlay Model Layer 2 MPLS VPN	• Supports any layer 2 protocol • Will transport already encrypted data, pre-MPLS • ISPs don't have to maintain additional complex customer routing tables	• Restricted to same data link protocol at both ends • Requires a full mesh of point-to-point interconnections between sites • Information not encrypted by MPLS VPN • Customer is responsible for all routing responsibilities
Peer Model Layer 3 MPLS VPN	• Not restricted to using the same data link protocol at both ends • Customers can be a member of more than one VPN • Allows for dynamic discovery of other sites for VPN	• Supports only IP traffic • Scalability problems for large deployments due to table sizes • ISPs have to maintain complex BGP routing tables • Information not encrypted by MPLS VPN • Customer has no control over the routing decisions

Table 1: MPLS VPN Comparisons [26][27]

4.0 GENERALIZED MULTIPROTOCOL LABEL SWITCHING (GMPLS)

There is an isomorphic input/output relationship between LSRs and OXC ingress/egress ports.[28] The parallelism between the two concepts leads to the idea of treating OXCs as optical LSRs by associating labels with optical wavelengths. By coincidence, both LSRs and OXCs maintain separate control and data planes. In so doing, it is possible to extend the common control plane concept of MPLS from electronic switching devices, like ATM switches and IP routers, to OXCs. Thus, network equipment developers coined the term “MPλS” to describe the concept of associating LSPs with OXC-provisioned optical links.

Generalized Multiprotocol Label Switching (GMPLS), which is a superset protocol including MPλS, was developed to support the benefits of MPLS over different types of transport networks such as spatial switching, optical wavelength switching, and time-division (SONET) switching. As new bandwidth demand increases and science approaches the physical limit of electronic switching, optical transport methods will proliferate industry, especially in core network backbones. In order to control the massive data flows and the diversity of traffic requirements, it is necessary to maintain a control protocol capable of handling this load and to efficiently interface with the optical switching components of the network. GMPLS was designed to provide the control mechanisms required to bridge the gap between electronic and optical intelligent traffic forwarding methods.

The NCS should closely monitor developments in the MPLS/GMPLS standards bodies to insure that NS/EP government communication priority is maintained. It is imperative that as voice, video, and data transport attains guaranteed QoS and are consolidated over a common infrastructure that there is preemptive capability for select priority traffic when/if the network becomes crippled or overloaded.

4.1 The Evolution of Optical Switching

Developments in optical communications lie at the heart of many advances in IP-centric communications. Introduction of fiber optic cables during the 1970s and 1980s created seemingly endless bandwidth. Carriers used simple fiber optic switches to restore broken fiber strands within spare fiber capacity in alternative cable routes.

By the mid-1990s, rapid Internet growth exhausted the supply of single wavelength transmission systems, leading to the deployment of WDM. WDMs multiplied fiber capacity by ten or even 100-fold. They also increased the complexity of managing the optical transmission system. OXCs appeared in the market for the purpose of reconfiguring lambda assignments within a WDM-multiplexed fiber strand and for restoring optical paths. Eventually, there will be optical packet switches that subdivide the bandwidth within a given lambda assignment.

More and more, optical switching is playing a role in the management of carrier network bandwidth. There is a growing need to integrate optical multiplexing and optical switching into the broader realm of network management. The resulting network management should give carriers greater control over their bandwidth resources, simplify network operation, and lower network operating cost. The need for better network management of optical resources is leading the development of GMPLS.

4.2 Method of Operation

GMPLS encompasses control plane signaling for multiple interface types. The diversity of controlling not only switched packets and cells, but also TDM network traffic and optical network components makes GMPLS flexible enough to position itself in the direct migration path from electronic to all-optical network switching. The five main interface types supported by GMPLS are:

- **Packet Switch Capable (PSC):** MPLS control of electronic packet transfer networks.
- **Layer-2 Switch Capable (L2SC):** MPLS control of electronic cell transfer networks.
- **Time Division Multiplexing Capable (TDMC):** Control of SONET/Synchronous Digital Hierarchy (SDH) based TDM multiplexers and cross-connects. Traffic is forwarded based upon time slot.
- **Lambda Switch Capable (LSC):** Wavelength/waveband based MPλS control of optical devices and wavelength switching devices, such as optical add/drop multiplexers (OADMs) and OXCs. Traffic is forwarded based upon wavelength/waveband.
- **Fiber-Switch Capable (FSC):** Spatial control of interface selection, automated patch panels, and physical fiber switching systems. Traffic forwarded based on port, fiber, or interface.[29]

These supported interfaces are controlled in unison by GMPLS. They are hierarchal in structure and traffic can be processed accordingly. Individual fiber, wavelength, time slot, and packet/cell type interfaces are supported by GMPLS, as shown in Figure 11.

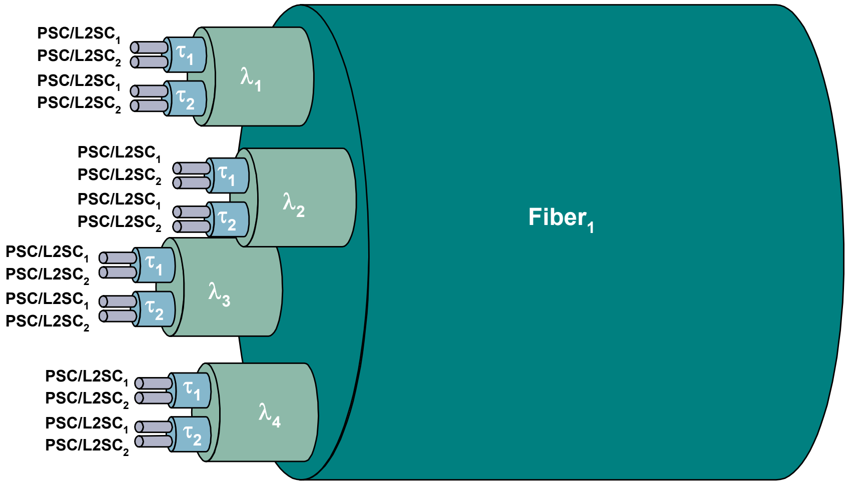
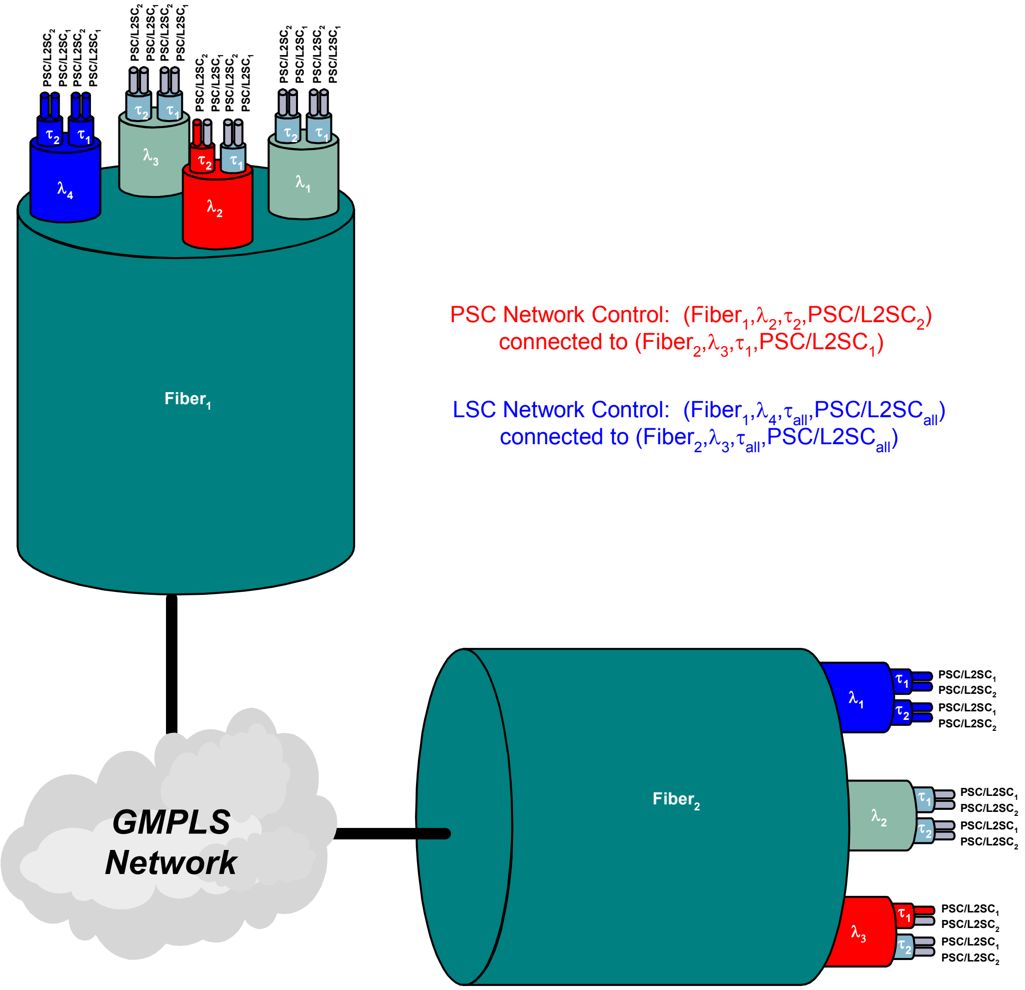


Figure 11: GMPLS Interface Types

Traffic can be switched through the network at any hierarchal level. Figure 12 depicts the control capability and flexibility of GMPLS. Notice that both PSC/L2SC and LSC traffic direction is shown.



PSC Network Control: (Fiber$_1$,λ_2,τ_2,PSC/L2SC$_2$) connected to (Fiber$_2$,λ_3,τ_1,PSC/L2SC$_1$)

LSC Network Control: (Fiber$_1$,λ_4,τ_{all},PSC/L2SC$_{all}$) connected to (Fiber$_2$,λ_3,τ_{all},PSC/L2SC$_{all}$)

Figure 12: Multiple Interface Type GMPLS Network Control

4.3 From MPLS to GMPLS

Extensions have been made to MPLS in order to support the different interface types discussed above. These proposed modifications are not in conflict with those specific to MPLS. In fact, much of the same protocol structure remains. Obvious modifications to the label have been made, and the necessity for a new method of managing the network links has been identified. Slight modifications have been made to the signaling (CR-LDP and RSVP-TE) and routing (OSPF and IS-IS) protocols of MPLS to support the multiple interfaces of GMPLS. Basically, the MPLS protocol has morphed into a more generalized structure to support a larger array of network technologies. MPLS/GMPLS may never dominate industry; however, it already has impacted network/protocol design philosophies. As we embark upon the next generation of network technologies, lessons learned from the implementation of and research on MPLS/GMPLS will forever shape future network architectures. As of the publication of this report, there was neither a standard, nor published RFC detailing the GMPLS protocol. The "Common Control and Measurement Plane" and "Multiprotocol Label Switching" Working Groups have posed recent Internet Drafts, currently under review by the IETF, outlining proposed modifications to evolve MPLS to GMPLS. Some of their research is discussed below.

4.3.1 Generalized Label

MPLS labels are embedded in the cell or packet structure for in-band control plane signaling. With the different interfaces it is impossible to embed label specific information, in terms of fiber port or wavelength switching, into the traffic packet structure. Therefore, virtual labels have been added to the MPLS label structure. These virtual labels are comprised of specific indicators that represent wavelengths, fiber bundles, or fiber ports and are distributed to GMPLS nodes via out-of-band GMPLS signaling.

GMPLS out-of-band signaling causes a control channel separation issue. With MPLS, the control information is found in the label, which is directly attached to the data payload. However, when you send the control information out-of-band, the label is separated from the data that it is attempting to control. GMPLS provides a means for identifying explicit data channels. Having the ability to identify data channels allows the control message to be associated with a particular data flow, whether it be a wavelength, fiber, or fiber bundle.

4.3.2 Generalized LSP

The handling of LSPs under GMPLS differs from that of MPLS. MPLS does not provide for bi-directional LSPs. Each direction LSP has to be established in turn. Under GMPLS, the LSP can be established bi-directionally. The traffic engineering requirements for the bi-directional LSP are the same in both directions, and it is established for both directions via only one signaling message. This allows for reductions in latency related setup time.

Another difference between MPLS LSPs and GMPLS LSPs is the ability to handle multiple adjacent links. The deployment of DWDM equipment has created a large number of individual connections between two adjacent nodes. GMPLS utilizes the concept of link bundling to handle these large quantity adjacent links. Link bundling treats the traffic of these like adjacent links as a single link. In order for the like adjacent links to be bundled, they must be on the same GMPLS segment, be of like type, and have the same traffic engineering requirements. This reduces the amount of link advertisements that need to be maintained throughout the network, thereby increasing the scalability of GMPLS.

Just as in MPLS label stacking, GMPLS labels only contain information about a single level of hierarchy. The difference for GMPLS is that this hierarchy can be fiber, wavelength, time slot, or packet/cell based. For instance, if a connection is desired from one PSC interface to another PSC interface, and the traffic traverses physically separate fibers, a unique LSP will have to be established for each level in turn. First, the FSC LSP, then the LSC LSP, then the TDMC LSP, and finally the PSC LSP would have to be established via GMPLS signaling. Figure 13 and Figure 15 depict this LSP establishment process for a network consisting of the nested components shown in Figure 14.

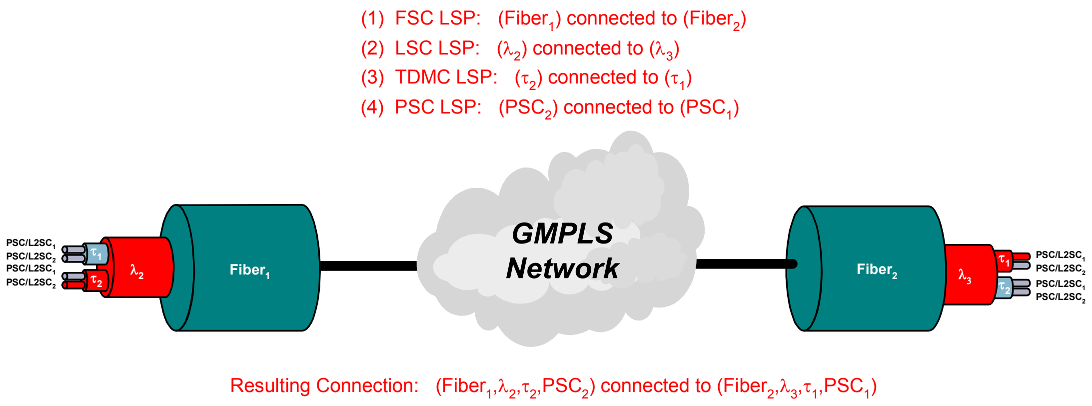


Figure 13: GMPLS LSP Hierarchy Establishment

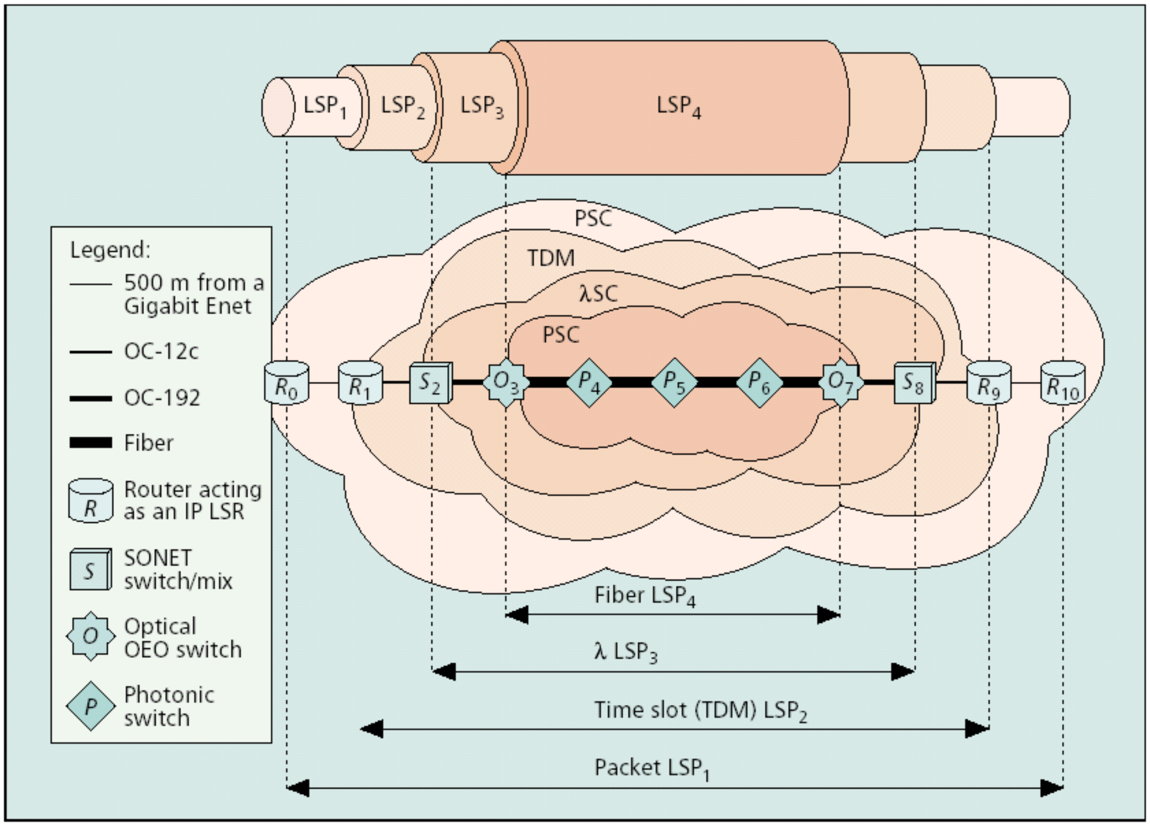


Figure 14: Nested LSPs within a Multi-technology Network [30]

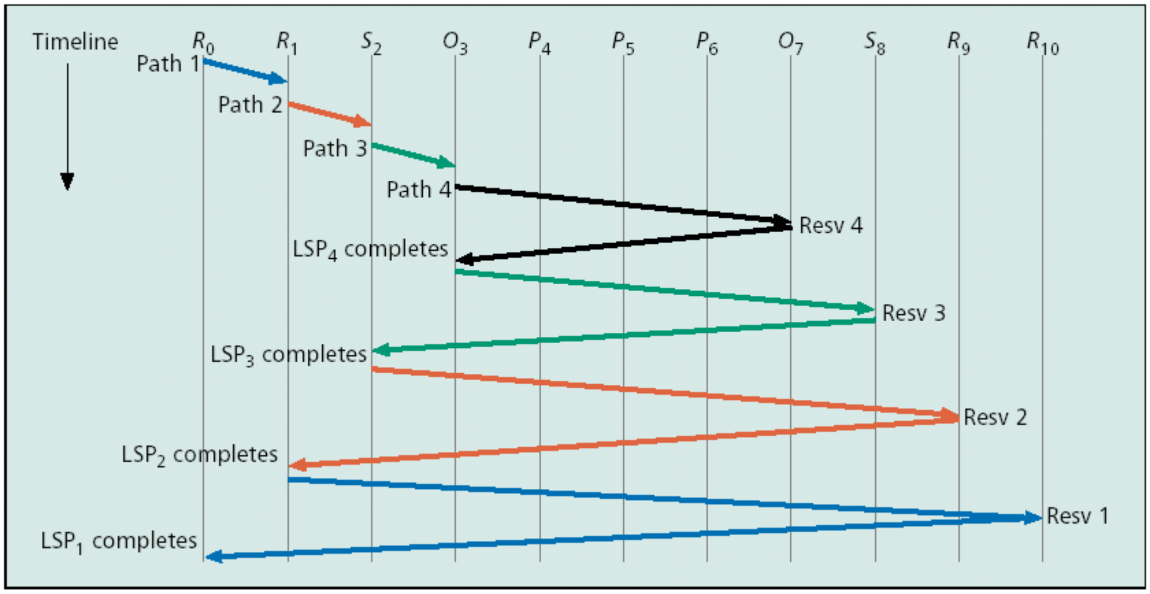


Figure 15: Nested LSP Establishment Across Multiple Technology Layers [30]

4.3.3 Link Management Protocol (LMP)

LMP runs within adjacent nodes. It provides link provisioning services and performs fault isolation. LMP automatically generates and maintains associations between links and labels for use in label swapping.[5] Automating the labeling process simplifies management and avoids the errors associated with manual label assignment.

LMP provides control channel management, link connectivity verification, link property correlation, and fault isolation. Control channel management establishes and maintains connectivity between adjacent nodes using a keep-alive protocol. Link verification verifies the physical connectivity between nodes, thereby detecting loss of connections and misrouting of cable connections. Link property correlation messages, called "LinkSummary" messages, correlate link properties like link identifiers, protection mechanisms, and service priorities. Fault isolation pinpoints failures in both electronic and optical links without regard to the data format traversing the link.

In order for these link bundles to be handled accordingly, GMPLS needed a method to manage the links between adjacent nodes. The Link Management Protocol (LMP) was developed to address several link specific problems that surfaced when generalizing the MPLS protocol across different interface types. Several Internet Drafts, current as of the writing of this report, address specifics of the link management protocol and are summarized in this section. The following is a list of the proposed responsibilities of the LMP as it relates to GMPLS.

- **Control Channel Management:** Establishment of a control channel is critical to GMPLS signaling. The maintenance of the control channel between adjacent nodes must be able to exchange information related to LSP establishment. Control channel management operates as the manager of control channel establishment and maintenance.

- **Link Property Correlation:** When link bundling occurs, GMPLS requires a way to verify that all traffic-engineering requirements are similar between like links of adjacent nodes. Link property correlation signaling performs the verification and performs the aggregation of like links.

- **Link Connectivity Verification:** Link connectivity verification is used by GMPLS to verify the connectivity between data links when the control channel is separate from the data link.

- **Fault Management:** Fault management provides the network with the ability to isolate faults down to the individual link.

4.4 Restoration and Reliability

Enhancements made to RSVP and LDP provide support for integration of the IP and optical control plane into the new protocol GMPLS.[30] These enhancements support several new features including protection and restoration.

GMPLS adds both network protection and restoration using span and path resiliency methods.[30] The resiliency methods consist of the following functions:

- fault detection
- fault localization
- fault notification
- fault mitigation using either protection or restoration schemes.

Fault detection occurs within the equipment nearest the fault (e.g., within WDMs or OXCs in the optical layer, within SONET multiplexers in the TDM layer, within ATM switches in the switching layer). LMP provides procedures for fault localization within both optical and optoelectronic networks. The protocol sends “ChannelFail” messages over control channels that are separate from the data plane. Separation of the control and data planes allows support for fault localization independent of the data transmission method, whether it happens to be ATM, SONET, WDM, or frame relay.

GMPLS mitigates failures using combinations of protection and restoration methods. GMPLS supports 1+1, 1:1, 1:N, and M:N protection and restoration methods. Figure 16 illustrates 1+1 and 1:1 protection. Figure 17 shows the use of 1+1 protection as a means of restoring a communication path.

GMPLS also supports both path and span restoration. GMPLS path restoration precomputes alternative restoration paths. In so doing, GMPLS expedites the rerouting of failed LSPs and improving the reliability of the LSP restoration, subsequent to a failure.

GMPLS provides fault notification for restoration with its addition of “Notify” messages within RSVP-TE as shown in Figure 18. Notify messages alert network nodes of LSP failures. LSP failures may occur within the data plane requiring rerouting of affected traffic, or they may occur within the control plane. In the later case, rerouting is not necessary or even desirable. Control plane failures may render support features like protection and restoration inoperative and require alternative measures or service provider intervention.

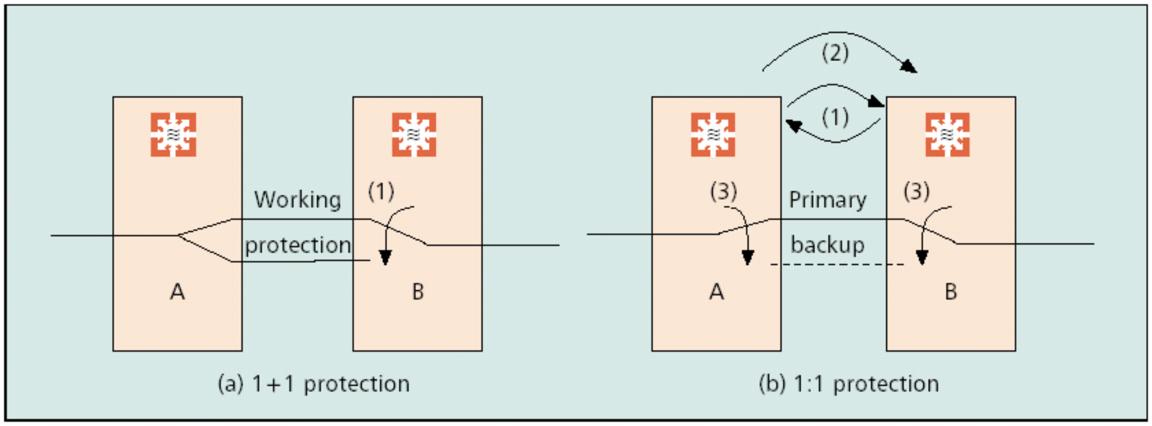


Figure 16: 1+1 and 1:1 Protection [30]

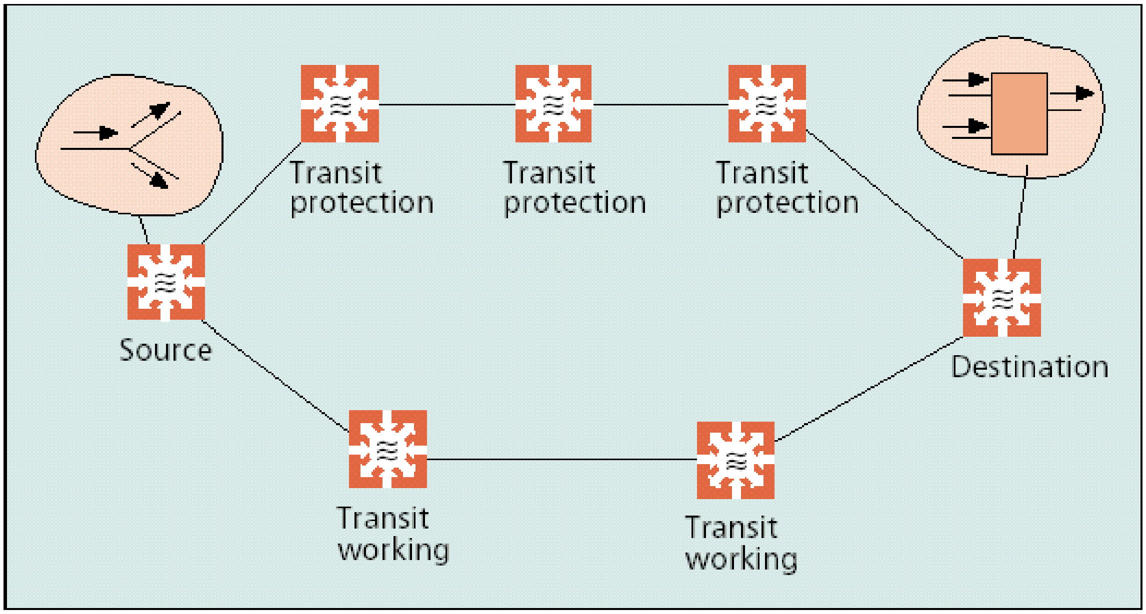


Figure 17: 1+1 Path Protection [30]

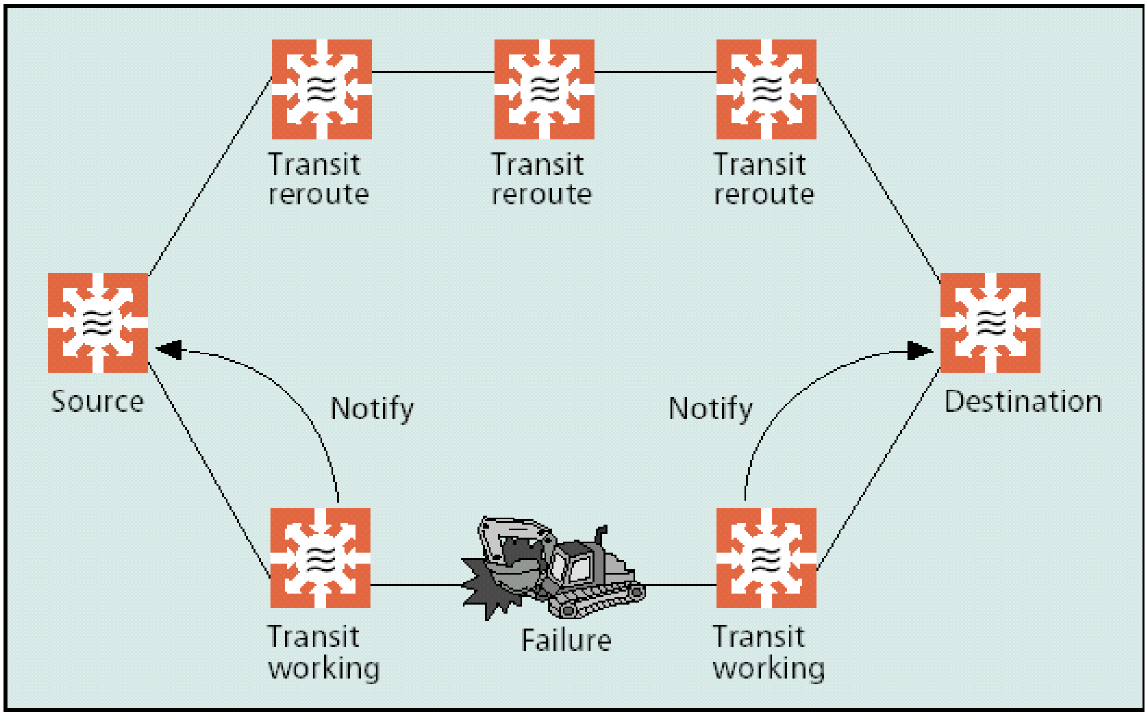


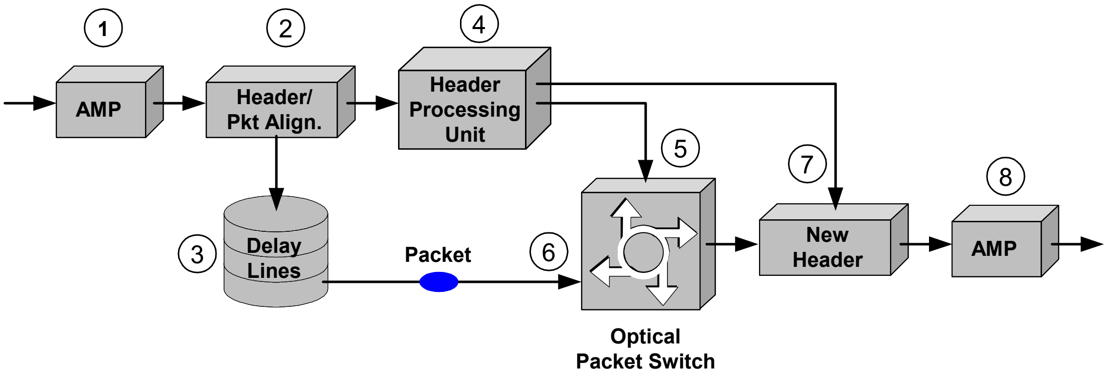
Figure 18: Path Restoration [30]

5.0 ADVANCED OPTICAL SWITCHING

Developments in the MPLS and GMPLS protocols only magnify the desire for all-optical data switching throughout the carrier networks. As research and development organizations, such as Telcordia, more thoroughly investigate the physical properties of optical components, there is a drive to migrate away from the electronic processing of the packet header. Current theoretical research into several forms of all-optical switching has improved existing optical backbone switching techniques; however, optical processing is still in its infancy. It is only through continued research that optical processing can be practically realized and implemented in network switching elements. Only then will the true benefits of an all-optical data network, with optical computation and establishment of optical routes, be realizable.

5.1 Optical Packet Switching

Optical Packet Switching (OPS) can be configured to operate on fixed and variable length packets. Slotted OPS deals with fixed length packets and requires the reconfiguration of the OPS prior to receiving the payload. Unslotted OPS can handle variable length packets; however, because the OPS is not configured prior to receiving the payload, contention issues can arise. Figure 19 depicts the flow of a slotted optical packet switch. First, the input signal is pre-amplified as necessary (①). Next, the packet header is reviewed and optional packet realignment occurs (②). The packet is then sent through a fiber delay line (③) to allow the header processing unit time to pre-configure the optical switch (④ and ⑤). The optical packet switch allocates the appropriate optical input to the appropriate optical output (⑥), a new header is attached (⑦), and the optical packet is amplified prior to retransmission (⑧). The process repeats and the switch is reconfigured each time. Currently, header processing and switch configuration is done in the electrical domain. Research is underway to append an optical header, based on advanced modulation techniques, to effectively provide all-optical table-referenced routing and switching functionality.[31]



① **Preamplification of optical input signal.**

② **Packet header review and optional packet alignment.**

③ **Delay on packet to allow for (4).**

④ **Header processing unit reads packet header.**

⑤ **Header processing unit pre-configures optical packet switch**

⑥ **Contention resolution provided by packet switch. Optical inputs sent to appropriate optical outputs.**

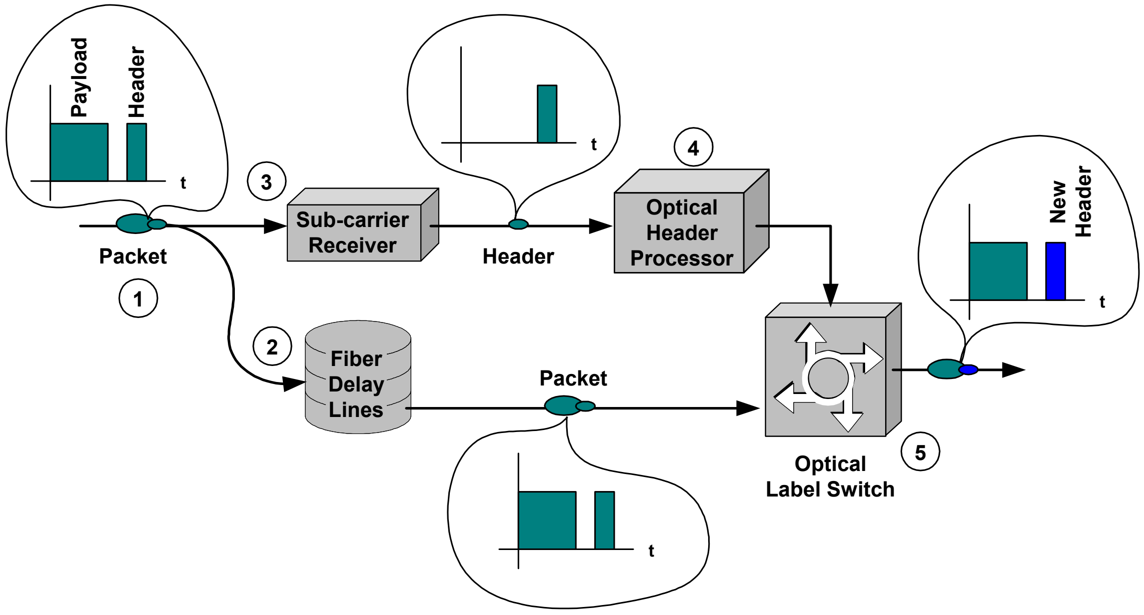
⑦ **New header written.**

⑧ **Optional power re-amplification.**

Figure 19: Slotted Optical Packet Switch Flow [31]

5.2 Optical Label Switching

Telcordia has conducted extensive research pertaining to Optical Label Switching (OLS). Optical Label Switching involves the use of sub-carrier multiplexing to append an optical header containing routing information to the optical payload. Figure 20 depicts the structure of an OLS node. First, the OLS node receives the packet. Both the payload and the header are on the same wavelength; however, the header is on a different sub-carrier (①). Next, the optical signal is split and received by a sub-carrier receiver (③) and fiber delay lines (②). The fiber delay lines delay the optical signal while the sub-carrier receiver forwards the optical header to the optical header processor. The optical header processor sets up the OLS prior to the packet arriving from the fiber delay lines. (④) Finally, the OLS receives the packet, strips off the old header information with a notch filter, appends a new optical header, and forwards the packet across the predetermined switched path (⑤).[9]



① Packet received by OLS node. Payload and header on same wavelength but header on different sub-carrier.

② Optical signal split and one side delayed by fiber delay lines.

③ While one signal is delayed, the other strips the header from the signal and forwards it to the optical header processor.

④ Optical header processor sets up the OLS prior to arrival of Payload.

⑤ OLS receives packet, strips off the old header information with a notch filter, appends new optical header, and forwards packet across predetermined switched path.

Figure 20: Optical Label Switching

OLS provides a means of transmitting the optical header in-band, on the same wavelength as the payload; this means that there is no need for the control plane to be separated from the data plane. The payload is completely optical through the OLS network, and therefore requires no electronic processing except, if necessary, at the edges of the network. Currently, the optical header must be processed electronically; however, research is underway to provide all-optical header processing, which will dramatically increase optical switching times. OLS is still in the initial development stage but could prove revolutionary to photonic switching networks. Figure 21 depicts the header format of OLS.

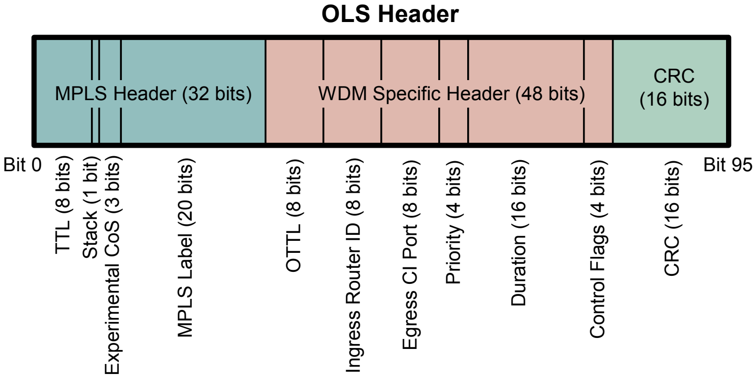


Figure 21: OLS Header Format [9]

Notice that the MPLS header structure is utilized with WDM specific setup information contained in an appended 48-bit header. With the addition of this header information, OLS has the ability to switch/route beyond the limitations of a traditional MPLS network. Telcordia is also researching optical label swapping, label address translation from IP-to-optical, as well as the optical control signaling to maintain and setup the optical connections.[32] The continuance of this research is critical to development of true photonic switching and routing.

5.3 Optical Tag Switching

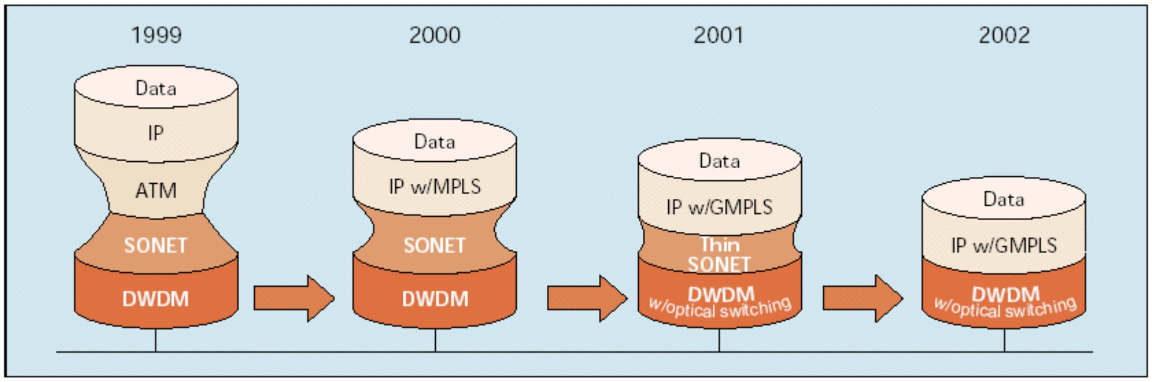
Optical Tag Switching (OTS) is similar to OLS in that both switching techniques keep the payload in the optical domain. The difference between the two is that OTS appends an optical tag containing simplified routing instructions to prevent the complicated network layer header from being processed at each node. These optical tags are appended by the ingress of the network and processed quicker at the intermediate nodes. Another difference is that the optical header is not separated from the payload for processing as in OLS.[33] Research on OTS is not widely published, and it is mainly discussed within the context of OLS.

5.4 Optical Burst Switching

Optical Burst Switching (OBS) is currently a more efficient optical switching scheme than OPS. The reservation of bandwidth is unidirectional, thereby eliminating the necessity of timely response messages. Aggregating packets in bursts of data allows for less processing overhead and increases the overall speed of the network. By utilizing bursts and unidirectional end-to-end bandwidth reservation techniques, OBS networks eliminate the need to process packets at intermediate network nodes and establish a direct network segment from source to destination. There are three different techniques to achieve OBS, In-Band terminator (IBT), tell-and-go (TAG), and reserve-a-fixed-duration (RFD).[31] NCS TIB 01-2, section 2.4.2, discusses these OBS techniques in greater detail. The current trend is for the development of OBS to continue to grow; however, once optical buffering techniques mature, OPS should become more prevalent than OBS, because OPS is based on the current electronic connectionless network switching paradigm.

6.0 TRENDS IN MPLS, GMPLS, AND ADVANCED OPTICAL SWITCHING DEVELOPMENT

Continued growth in data networks will make IP the dominant data forwarding method. The authors in [5] foresee the eventual consolidation of the four network layers into as few as two layers consisting of GMPLS and DWDM. They foresee GMPLS bypassing the ATM and SONET layers. However, their time schedule shown in Figure 22 for the conversion is highly unlikely in that it predicts the consolidation to be complete by 2002. The service providers cannot convert their systems in such a short time frame, especially during the current economic doldrums.



© 2001 IEEE

Figure 22: Conversion to MPLS and GMPLS Forecast [5]

Development of all optical switching techniques is still in infancy. The necessity for optical processing of, for example, optical labels, is of high interest in the research community. Telcordia is leading the advanced research in this area, and breakthroughs have been made; unfortunately, it will take time for these breakthroughs to materialize into practical implementations for use by network engineers.

6.1 Early MPLS Adopters, Cost, and Availability

Even so, there have been a few early adopters of MPLS amongst the carriers. MPLS services are available, albeit with several limitations.

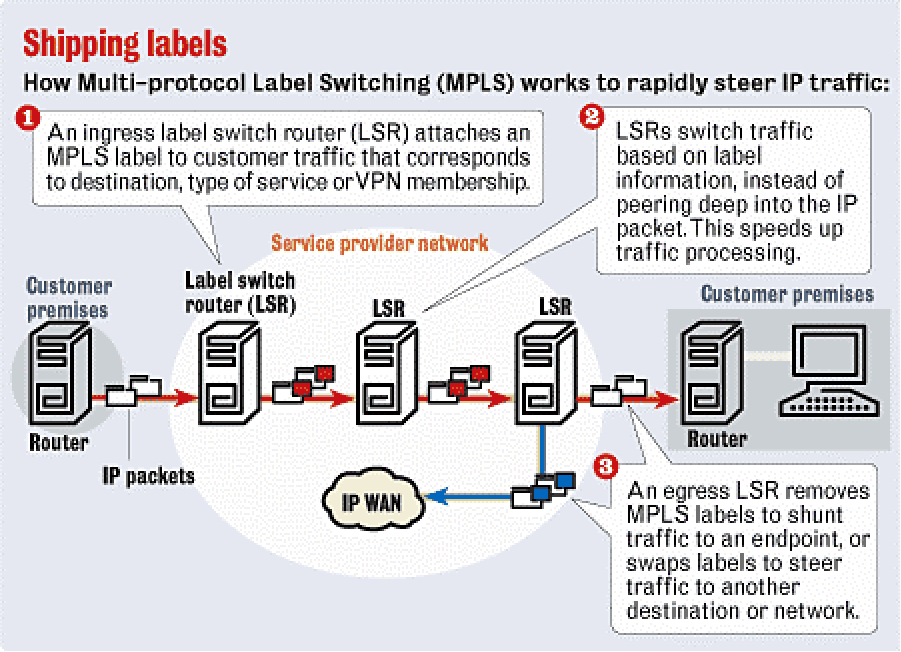
Network Magazine issued a request for information (RFI) for multinational MPLS network services as a way of gauging the availability and cost of MPLS services worldwide.[34] The RFI specified that the proposed network carry a combination of data and voice traffic between major cities in the US, Great Britain, and Western Europe. American Telephone and Telegraph (AT&T), Global Crossing, Equant, Infonet, and Cable and Wireless (C&W) responded with network designs and price proposals. Of those carriers that responded to the RFI, only AT&T and Equant offered MPLS services. Global Crossing, Infonet, and C&W offer ATM-based services in lieu of MPLS services.

Evaluation of the proposals shows that MPLS services currently have less international coverage, limited network access options, and lack the technical features and operational maturity of ATM services. MPLS services were three times more expensive than equivalent ATM services. Network operators were unable to offer exhaustive traffic analysis as a part of their network operations. Only Equant claims to have extensive international coverage with access to over 200 countries. AT&T offers much less extensive international coverage.

Only Equant carries both voice and data over the same MPLS network. AT&T separates voice traffic from data traffic at the network edge. Data traffic travels over their MPLS network via Cisco System MPLS LSRs. Voice traffic travels over AT&T's frame relay network. AT&T says their LSRs lack necessary voice compression features for handling voice traffic efficiently. There were questions regarding the ability of AT&T's voice services to scale gracefully to meet growing voice traffic demand. Equant claims their Cisco Systems' LSRs are equipped with voice compression and send the traffic over a common MPLS network. Differences in the two MPLS carriers' network designs highlight the lack of consistency in MPLS network services.

None of the responding carriers offer direct customer access to their MPLS LSRs and the MPLS protocol. MPLS access from the customer premise to MPLS networks is not available. MPLS carriers currently offer only frame relay, ATM, or X.25 access to their MPLS services. Access to AT&T's network is primarily frame relay or ATM. Equant network access is via X.25 protocols. In either case, Equant and AT&T adapt enterprise traffic into a MPLS VPN network as shown in Figure 10.

The lack of direct MPLS access reveals a significant aspect of MPLS deployment within the carrier networks. For the foreseeable future, enterprise customers will connect to carrier networks using ATM, frame relay, or X.25 protocols. MPLS will be an interior routing protocol used within the service provider networks. Figure 23 shows the carrier's local access network delivering enterprise IP traffic to the MPLS network using conventional ATM, frame relay, or X.25 protocols. The carrier's network edge devices adapt the customer's traffic to the MPLS protocol.



Shipping labels

How Multi-protocol Label Switching (MPLS) works to rapidly steer IP traffic:

① An ingress label switch router (LSR) attaches an MPLS label to customer traffic that corresponds to destination, type of service or VPN membership.

② LSRs switch traffic based on label information, instead of peering deep into the IP packet. This speeds up traffic processing.

③ An egress LSR removes MPLS labels to shunt traffic to an endpoint, or swaps labels to steer traffic to another destination or network.

Reprinted with Permission of Network World

Figure 23: Customer Access to MPLS [35]

ATM continues to be the protocol of preference for the majority of the carriers. Three of the five responding carriers use ATM in lieu of MPLS for their core network. It remains to be seen whether a larger number of carriers will adopt MPLS core networks and whether the MPLS protocol will extend to customer access. Philosophically, MPLS is an interior network protocol. It is not necessarily the intention of the MPLS developers to extend the protocol to enterprise networks. If so, then the enterprise will not be the driving force in its deployment. Carriers and other service providers are the key beneficiaries and the targeted customer group for MPLS.

6.2 ATM Solutions Compete for IP Packet Forwarding

Internet routing traditionally is hop-by-hop. Exponential growth in the Internet is making hop-by-hop routing impractical.[36] ATM is a popular method for on-demand connections between network endpoints.

Most efforts to route IP traffic across ATM core networks involve decoupled routing and signaling between the IP and ATM layers.[36] Decoupled routing and switching within the network creates inefficiencies and complicates management tasks. Current IP over ATM implementations take no advantage of QoS within the ATM network.[37] Efforts are underway to improve the integration of IP routing and ATM switching.

IP over ATM is the subject of standardization efforts in the IETF, ATM Forum, and ITU-T. The ITU-T is considering enhancements to the ATM signaling to better support IP traffic in standards. For example, Q.6, Q.13, and Q.20 support MPLS signaling functions.

At the same time, ATM Forum is working on Private Network-Network Interface (PNNI) augmented routing (PAR) and Integrated-PNNI (I-PNNI) in a two-pronged effort to improve IP over ATM. Integrated PNNI takes an ambitious approach by enhancing the PNNI protocol to carry IP and ATM routing information between the ATM and IP layers. It creates a tight integration between IP and ATM routing functions. I-PNNI protocol adds hop-by-hop routing to create a multi-layer routing protocol.

The ATM Forum PAR protocol is a more conservative alternative to I-PNNI. PAR implements an instance of PNNI signaling within the network edge router along with their OSPF, RIP, and other IP protocols. The PNNI instance gives the router visibility into the ATM topology. PAR creates the ability within a router to establish SVCs for direct cut through routing of IP traffic between routers on the edge of the ATM network. It permits the IP router the ability to specify QoS for IP traffic. PAR-equipped routers make SVC connections across the ATM network and send traffic across the SVC network shortcuts. In different ways and with different levels of implementation complexity, I-PNNI and PAR provide a more effective signaling interface for establishing cut-through connections within an ATM core network.

6.3 Arguments For and Against Carrier Adoption

Critics of MPLS VPNs point out the lack of encryption within MPLS-based VPNs. MPLS VPNs do not encrypt information. Information sent to the wrong person is easily readable. Detractors claim that MPLS VPNs could “leak” sensitive information. They also warn carriers that they may be overwhelmed trying to manage BGP routing tables.

Two AT&T Labs researchers, Steve Bellovin and Randy Bush, are skeptical about MPLS as a next generation network protocol.[27] MPLS VPNs have security weaknesses and may not be scalable from a management standpoint. RFC 2547 requires carriers and ISPs to manage special BGP routing tables for each MPLS VPN. Network operators must store the tables at every location with VPN access. Carriers and ISPs may be faced with managing thousands of tables.

The RFC 2547 BGP/MPLS VPN protocol dedicates paths across a carrier network for the purpose of creating customer VPNs. RFC 2547 uses BGP to distribute MPLS routing information throughout the network. The number and size of the BGP routing tables become large as the network scales upward in size. Despite its detractors, Cable & Wireless and Global Crossing (contingent upon the outcome of its bankruptcy restructuring efforts) will deploy RFC 2547-based MPLS VPNs.

Bellovin and Bush recommend that the core of the network be simple, fast, and dumb. Complexity and intelligence should exist along the edge of the network where traffic densities are low and application-specific adaptations are regular occurrences. MPLS tends to distribute complexity and intelligence throughout the network. The relatively primitive state of wide bandwidth optical switching technology does lend itself to complex routing or processing functions. Thus, it is preferable to keep complexity and intelligence along the network edge where traffic densities are light and sophisticated electronic switching is prevalent. Their worry is that the addition of complexity within the network will limit scalability of MPLS networks to very high optical bandwidths.

In many ways, carriers need network control protocols for VPN data networks comparable to the SS7 protocol used in telephony networks. The new protocol should route traffic quickly, restore services around network faults, and be a platform for value-added services. The protocol should provide a common control plane over which dissimilar network data planes can be unified into a cohesive service. The candidate protocol for creating a common data-centric control plane protocol is GMPLS.[3]

If it lives up to all of its proponents' promises, GMPLS will do much more within data networks than is accomplished through SS7. GMPLS will automate provisioning across ATM, SONET, OXC, and fiber optic data planes. It will eliminate manual, error prone, and oftentimes tedious manual provisioning methods.

6.4 Trends in Adoption of MPLS and GMPLS

The expected migration to IP protocols, including MPLS and GMPLS, will be gradual. In the meantime, network equipment makers continue to emphasize and enhance their product lines of SONET and ATM equipment for use in service provider networks.[38]

Carriers continue to invest billions of dollars in network improvements, but these investments are not currently being placed in the construction of new services.[39] Most of the new carrier investments strive to reduce cost and improve returns on existing, revenue producing services including voice, ATM, and frame relay. New investments reduce floor space occupancy, reduce power consumption, simplify management, and reduce or eliminate staff training requirements.

Incumbent carriers over-invested $40 billion from 1998 through 2001 in construction and implementation of network capacity.[39] Those emerging carriers that appeared after the Telecommunications Act of 1996 spent a whopping $20 billion in 2000 alone. Many of the emerging carriers are either bankrupt or facing the threat of bankruptcy (e.g., Global Crossing). All carriers are restructuring their investments in response to the 2001 economic downturn and major reductions in revenues. AT&T, SBC Communications, Qwest Communications, WorldCom, and Verizon are keeping 2002 investments at or below 2001 levels.

Regional Bell operating companies (RBOCs) continue to invest in SONET and WDM to sustain voice services, expand their existing data services, and improve fiber usage efficiency. Many carriers are investing in packet telephony, i.e., VoIP, equipment in effort to consolidate their voice and data networks. They are shunning voice-only investments in SONET. They are avoiding investments in advanced IP services equipment and in the new generation of MPLS edge and core network equipment.

6.4.1 Carrier Industry under Reality Check

Proponents of MPLS frequently speak in terms of a complete "fork-lift" upgrade approach to installing MPLS within the carrier networks.[36] A massive replacement of carrier equipment is financially and logistically impractical. Any enhancement of carrier network technology will occur gradually over time using technology that both adds new value-added services and continues to support revenue-producing legacy equipment.

Incumbent carriers continue to derive revenues from their SONET and ATM traffic. ATM and SONET equipment represents the preponderance of the electronic communications equipment within carrier networks.[38] For now, carriers are focusing their investments in proven equipment and at choke points in their network. Capital spending is largely curtailed to that of meeting network traffic demand for existing services. The authors do not expect carrier equipment spending to recover to pre-recession levels until mid-year 2003.

Constructing the "information superhighway" cost nearly $2 trillion. Large portions of this huge investment have been lost during the 2001 recession along with the aspirations of many would-be "dot.coms" and upstart carriers. In the meantime, there is a glut of network capacity that may last for years.[40]

Financial woes are overtaking the carrier industry and all of its equipment suppliers. Carriers like Global Crossing, Qwest Communications, Level 3 Communications, Sprint, and William Communications are facing major restructuring or even bankruptcy.[41] Competitive local exchange carriers (CLECs) vanished from the marketplace with the latest economic recession. Many of the interexchange carriers (IXCs) are in deep financial difficulty. Incumbent local exchange carriers (ILECs) are not spending capital on new services. The vacuum created by the economic downturn is putting many equipment manufacturers out of business.

The carrier industry is suffering from the boom hangover of the 1990s, leaving them with the financial burden created by over-construction of fiber optic cables and over-investment in equipment. Many of the equipment manufacturers like Cisco Systems and Lucent are left with unpaid accounts receivable and inventories of used equipment with no immediate prospects of new equipment sales.

The combined effects of deregulation mandated by the Telecommunications Act of 1996 and euphoria over rapid growth in Internet traffic led many to invest heavily into communications technology. The telecommunications industry borrowed over $1.2 trillion to invest in fiber optic cables and network equipment. Network capacity grew rapidly without a corresponding increase in revenues. Consequently, many telecommunications companies are either restructuring or going out of business. Many companies are firing employees and selling assets at huge losses. Price wars plague the industry, reducing bandwidth revenues by as much as 100-fold. Failures of many dot.com carriers, coupled with their heavy investments in capacity expansion, left them holding large amounts of excess capacity and a heavy debt burden. Some estimates say that only 10 percent of the installed global fiber capacity is in use.

6.4.2 Local Access Is Still a Service and Revenue Bottleneck

There are basic economic problems impeding growth of high bandwidth related revenues and growth in new subscribers.[40] Many small businesses and residences do not have high-speed access to carrier networks, leaving carriers without the means to deliver excess capacity to new customers. The cost of upgrading local access, often called "the last mile," continues to hamper deployment of Integrated Services Digital Network (ISDN) and DSL services.

Cable TV companies are faring better in their deployments of cable modem services to new subscribers. High-speed cable access to the Internet grew 12% last year, reaching 7.2 million subscribers by 4th quarter 2001, according to the National Cable and Telecommunication Association. The two biggest DSL providers, AT&T Broadband and SBC Communications, only have a total of 2.8 million DSL subscribers. Cable modems benefit greatly from the fact that residences and small businesses can use the same coaxial cable to purchase video, high-speed Internet, and even telephone services.

The cable television (CATV) industry is developing and enhancing CableHome, PacketCable, and data over cable service interface specification (DOCSIS) standards.[42] DOCSIS codifies the connection of customer premise cable modems to hybrid fiber-coax (HFC) networks. CableHome defines methods for distributing packet-based services within the home. CableHome adds firewalls, DHCP protocols, QoS, and TFTP services. PacketCable defines methods for interconnecting cable TV networks to the Internet. PacketCable adds dynamic QoS, allowing variable-on-demand bandwidth provisioning for voice, data, and IP gaming applications. These standards may lead to unified residential communications systems that encompass video-on-demand, telephony, and high-speed Internet access.

6.4.3 Changing the Installed Base Takes Time

Deployment of GMPLS cannot take place overnight. The massive installed base of multilayer networks dictates a gradual migration, using GMPLS where it can be integrated with legacy systems and when it can produce real benefits to the carrier.[3] The first step towards a unified GMPLS control plane may be the implementation of a unified service provisioning system with “point-and-click” features for service provisioning engineers. A simplified and automated provisioning system would reduce provisioning cost, reduce provisioning delays, and improve service reliability. A subsequent addition of UNI would permit network edge devices like routers and ATM switches to request connectivity on-demand. On-demand provisioning would add value to the service provisioning process and eliminate more provisioning cost.

However, on-demand provisioning requires massive changes to carrier billing data collection and processing systems. The lack of adequate billing systems sidelined ATM SVC services and restricted ATM-based service to those that use PVCs.[43] It is not clear that the carriers will be successful in creating scalable and flexible billing systems to match a highly scalable and extremely flexible on-demand provisioning system made possible by GMPLS, MPLS, ATM, or other on-demand provisioning protocols.

6.5 Outstanding Issues for MPLS and GMPLS

MPLS traffic-forwarding efficiency is superior to traditional hop-by-hop packet forwarding methods.[44] MPLS data forwarding resembles that of ATM, frame relay, and X.25 networks. It shares improved security with these networks due in large part to its connection-oriented behavior. Many of these improvements hinge upon the widespread use of protocols like OSPF and IS-IS.

OSPF maintains complete awareness of network topology, which includes all nodes and links. Traffic engineering enhancements make OSPF aware of traffic parameters associated with the nodes and links.

However, OSPF does not extend topology information across network domains. Therefore, there is a lack of traffic engineering across domains.[44] These limitations allow OSPF to scale to large, multidomain networks, but may lead to suboptimal connections across domains. The lack of signaling across carrier domains will lead to routing problems between competing domestic carriers and between international signatory carriers.

OSPF and IS-IS are complex protocols to design and implement. It takes large amounts of router CPU capacity to compute new routes.[45] They have an added disadvantage of flooding the network with link state advertisements (LSAs), especially during frequent network outages. The quantity of LSA messages and the computational intensity of route computation may be limiting factors in the ability to scale MPLS and GMPLS into large networks.

MPLS supports both unicast and multicast data forwarding, but there remains a number of issues to be resolved before MPLS can support multicast on a broad scale:

- MPLS lacks the ability to combine multicast trees with different multicast destination addresses on the same LSP.
- MPLS cannot establish shared multicast trees in ATM or frame relay networks.
- It lacks efficiency in mapping a Layer 3 point-to-multipoint tree to a Layer 2 point-to-multipoint tree in a changing network environment.
- MPLS cannot create many merge points for bi-directional shared trees.
- MPLS mechanisms are missing for constructing multicast distribution trees with QoS constraints.

There are many challenges ahead regarding the ability of MPLS to inter-network with ATM and frame relay networks.[44] It is essential that MPLS inter-network with ATM and frame relay because of the large installed base of ATM and frame relay equipment. Moreover, ATM and frame relay are the backbone of the service providers' revenue-producing networks.

The ATM Forum and the MPLS Forum will jointly address issues regarding the inter-networking of their ATM and MPLS protocols.[46] They will consider signaling and routing between ATM PNNI and MPLS protocols, service inter-networking, and assuring QoS and traffic guarantees across intermediate MPLS networks. The MPLS, ATM, and Frame Relay Forums are working on inter-networking specifications. Even so, work remains to create solutions practical to carriers that allow MPLS, frame relay, and ATM networks to operate together in an efficient, manageable way.

From a business standpoint, carriers generally lack appropriate billing and traffic engineering systems to support bandwidth on-demand services.[43] Two notable exceptions are the public telephone and cellular telephone networks. Telephony services have billing systems that support on-demand use of the carrier network. For data services, carriers deploy the overlay VPN model and bill based upon a point-to-point, PVC service fee.

The lack of a carrier bandwidth billing system left bandwidth on-demand protocols like ATM SVCs languishing without significant support within ISP networks. Consequently, carriers continue to use PVCs within ATM networks capable of bandwidth on-demand provisioning. It is not clear how the advent of MPLS and GMPLS will resolve the absence of billing systems capable of recovering revenue from bandwidth on-demand services.

6.5.1 The State of the Standards

There are over 100 standards in draft form by the IETF, ITU-T, Institute of Electrical & Electronics Engineers (IEEE), and Optical Internetworking Forum (OIF) attempting to provide new methods for operating communications networks.[47] Many of these protocols attempt to redefine network services in terms of wide bandwidths on-demand. These new protocols would replace the current paradigm of fixed bandwidth services provisioned for a specified lease period (e.g., month, year).

The new standards pit the Ethernet-IP paradigm of enterprise networks against the SONET paradigm of the largely voice-based carrier networks. Enterprises want simple, easy to manage networks where bandwidth efficiency and manageability are not the primary concerns, while carriers need highly efficient, manageable networks. Carrier network requirements generally involve more complexity than is manageable by an enterprise.

The advent of optical networks and growing demand for wide bandwidth services is forcing the needs of Ethernet-IP users upon the carriers. On one hand, Ethernet-IP users promote the use of GMPLS as a natural extension of IP-centric designs into carrier network interfaces. GMPLS supports allocations of wide bandwidths on-demand to meet developing capacity needs. SONET-centric users are promoting the use of an ASON. Each approach follows its own set of standards and leads to a different network design.

GMPLS lends itself to a peer-to-peer network design where every switching device, called a “label switch router” (LSR), is aware of the network’s topology and resources. Peer-to-peer networks divulge large amounts of network design information. Many carriers resist sharing network topology and resource information with customers or with one another.

From the public service provider point of view, carriers favor an overlay network design. The overlay network design employs UNIs and network-to-network interfaces (NNIs). Overlay network designs using UNIs and NNIs share necessary user provisioning and carrier capacity exchange information without divulging large amounts of carrier proprietary network information.

To date, GMPLS only supports a peer-to-peer network architecture where all LSRs are aware of the entire network topology and resources.[47] The OIF is working on a GMPLS UNI to address the need for overlay networks across carrier infrastructure. Thus far, the draft standard provides for adding, deleting, and obtaining status on connections via the GMPLS UNI. There remains the need for additional features like interdomain signaling and alarm signaling.

SONET's inability to efficiently carry Ethernet traffic lies at the heart of this debate. SONET wastes large amounts of expensive bandwidth when attempting to carry 100 Mbps Ethernet traffic over a 155 Mbps OC-3 SONET channel. Worse yet, SONET does not work efficiently with the multiple wavelengths provided by WDMs. Instead, SONET is a single wavelength communications protocol. It does not manage multiple wavelength communications channels. SONET does not support on-demand allocations of bandwidth. It lacks UNI and NNI signaling necessary for rapid, automatic provisioning of services. It relies on subscription-based provisioning and manual interaction with its provisioning subsystems. The fixed provisioning methods of SONET work well within a voice network where switching occurs at higher network layers. However, it does not support the network requirements of enterprise users and IP-centric networks, especially if they rely on Ethernet as the underlying network transmission method.

The massive transition from voice communications to IP-centric communications heightens the dilemma and creates a need for better support of IP-centric services. Growing bandwidth demands place the solution beyond the reach of current SONET technology. SONET does not scale well above OC-3 services and leads to costly investments in equipment for the service providers. SONET's lack of scalability makes support of wide bandwidth, Gigabit Ethernet or 10 Gigabit Ethernet traffic impractical.

The carriers cannot readily accept and distribute Ethernet traffic across their metropolitan area networks (MANs) or the WANs. Ethernet lacks QoS controls and methods for restoring traffic following network failures.

6.5.2 North American MPLS and GMPLS Codification Efforts

Several North American organizations are working on MPLS, GMPLS, and associated standards.[48] The IETF led much of the work that consolidated the many alternatives proposed by Cisco Systems and other industrial groups.

IETF is an international standards body devoted to the promulgation of Internet-centric and IP-centric communication standards.[3] Enterprises rely heavily upon IETF standards for their IP-centric networks. IETF is largely responsible for the standardization of MPLS for electronic network layers. It recently turned its attention to the development of GMPLS as a means of extending the MPLS concept to the optical layers of a network.

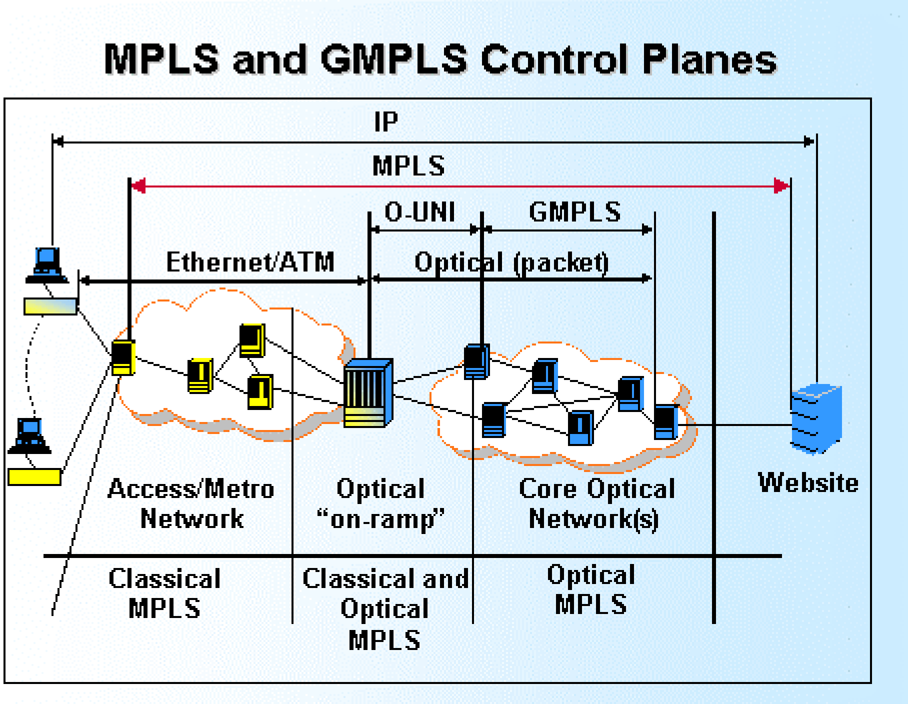
The IETF is currently working on the formalization of GMPLS, which is still in draft form. Six IETF working groups are defining different aspects of MPLS and GMPLS. The IETF frequently incorporates contributions from industry and other forums such as OSDI, OIF and the ITU-T.

Optical Domain Service Interconnect (ODSI) developed a GMPLS UNI allowing routers, add-drop multiplexers (ADMs) like SONET equipment, and ATM switches to request light paths on-demand. ODSI draft standard is complete and is now under consideration by the IETF and ITU-T.

The OIF has the more ambitious goal of developing interoperability and physical interface standards between optical systems. The OIF scheduled interoperability tests during the second quarter 2001.[48] Its work on optical signaling methods is ongoing and remains in draft form. The OIF is working closely with IETF and expects much of its work to be codified within the IETF standards.[3]

The work of the OIF is complementary to those of the ITU-T. The OIF's emphasis on network overlay model concepts like UNI and NNI fit within the overall philosophy of ITU-T architectures.

Figure 24 gives a conceptual illustration of the OSDI and OIF concept of a GMPLS UNI connecting the MPLS and GMPLS control planes in overlay model fashion. Ethernet and ATM constitute the access network layer. MPLS controls LSP provisioning within the ATM portions of the carrier network. A GMPLS UNI coordinates LSP provisioning and LSP nesting between the MPLS and GMPLS control planes. GMPLS provisions optical LSP using OXC and WDM systems within the carrier's optical core network.



© Scott Clavena, "Optical Signaling Systems," Light Reading, Inc., January 28, 2002
http://www.lightreading.com/document.asp?site=lightreading&doc_id=7098&page_number=1

Reprinted with Permission of Light Reading, Inc.

Figure 24: MPLS and GMPLS Control Planes Using an Overlay Model [3]

6.5.3 A Pending International Standards Verdict

The ITU-T is the foremost body for the establishment of international communications standards.[3] It is the body that most countries and carriers turn to when seeking interoperable communication and a strategic direction for network architectures.

ITU-T takes a deliberate, even painstaking view toward global network architectures. It looks beyond just IP-centric architectures to include voice, multimedia, and optical architectures. ITU-T establishes a vision for global network architectures and only then defines standards that support the strategic vision.

The ITU-T's view of communications is truly international. Its "one country, one vote" manifesto creates a forum in which many countries can contribute, be heard, and in which no one country or region can dominate.

Each country has at least one international carrier and one or more domestic carrier. In the case of the US, Great Britain, and Japan, there are many international and domestic carriers. All of the carriers must rely on a uniform set of international communications standards in order to exchange traffic between each other within a country and across borders with carriers in other countries. The carriers rely on the ITU-T as their most trusted source for strategic network architecture design and protocol specifications.

ITU-T architectures must support many different network domains operating within many different sovereign nations. An overlay model respects national borders and domestic policies of sovereign network domains. It is unlikely that the ITU-T would change course to support MPLS or GMPLS specifications based upon a peer network model. A peer model with its open sharing of network information will surely raise national economic or security concerns for many countries, including the United States.

The ITU-T and ANSI are working together to create an overlay signaling protocol for optical networks using a client-based approach under the auspices of the Automatic Switched Transport Network (ASTN) and ASON standards.[47] Clients like Ethernet switches, and routers would request connections through the optical network via a UNI in much the same way as a telephone caller requests connections across a telephone network. Service providers interchange connections using a corresponding NNI.

The new ASTN standards will support hybrid connections called "soft provisioned connections" (SPCs). Much like the ATM soft permanent virtual circuit (SPVC), the SPC uses fixed access connection to connect a subscriber into the ASTN and switched connection across the ASTN to complete the connection between the two, fixed access connections.

The lack of ITU-T endorsement of MPLS and GMPLS calls into question the viability of MPLS and GMPLS.[34] Carriers must provide international services and interface with foreign networks to provide a full suite of services. After all, most corporations and government agencies have foreign offices as reflected in Network Magazine's RFI. Targeting service providers with a protocol technology like MPLS and GMPLS without international standards body support is risky. It is unlikely the foreign carriers will adopt a protocol developed in the North American market without ITU-T sanction. MPLS and GMPLS could die a sudden death without the international communications community support.

The ITU-T may or may not choose to sanction MPLS or GMPLS.[3] It is considering several options under a concept called the "Architecture for Optical Transport Networks (AOTN)," ITU-T Standard G. 872. AOTN describes the fundamental aspects of the ITU-T's vision for optical networks. Work related to the development of the AOTN falls within a set of interrelated standards described in Table 2. Ultimately, the ITU-T may choose an alternative approach and may ignore MPLS, GMPLS, or both.

ITU-T Standard Identifier	Description
G.709 (2001)	Network node interface for the SDH
G.705 (2000)	Characteristics of Plesiochronous Digital Hierarchy (PDH) equipment functional blocks
G.707 (2000)	Network node interface for the SDH
G.959.1	Physical layer interfaces for the optical transport network (OTN)
G.783 (2000)	Characteristics of SDH equipment functional blocks
G.8030 (2000)	Architecture of transport networks based on SDH
G.8050 (2000)	Generic functional architecture of transport network
G.871 (2000)	Framework of Optical Transport Network Recommendations
G.872 (1999)	Architecture of Optical Transport Networks defines an optical transport network consisting of optical channels within an optical multiplex section layer within an optical transmission section layer network. A unified control plane manages the optical channels.
G.8080	Describes the reference architecture for the control plane of the Automatically Switched Optical Network (ASON). ASON supports the requirements for a client-server model of optical networking. This recommendation describes the set of control plane components that are used to manipulate transport network resources in order to provide the functionality of setting up, maintaining, and releasing connections. It creates the capability within the optical network for a network operator to bill for connections and, based on the parameters of the class of service requested for the connection, select the connections with the type of protection or restoration required to meet the class of service.
G.7713/Y.1704	Distributed Call and Connection Management
G.7714/Y.1705	Generalized Automatic Discovery Techniques
G.7712/Y.1703	Architecture and Specification of Data Communication Network

Table 2: ITU-T Architecture for Optical Transport Networks Standards [3]

For now, MPLS and GMPLS are largely North American standards developments. Therein lies the risk to early adopters of these North American standards There are many examples of prior standard-setting initiatives that have failed for lack of ITU-T sanction. For example, frame relay developed in North America as a replacement to X.25 packet switching protocols. Frame relay never achieved ITU-T standards status. Instead, the ITU-T-sanctioned ATM protocol quickly upstaged frame relay in the carrier networks. Frame relay persists as a North American service to enterprises that choose to use it, but almost all carriers adapt frame relay traffic to ATM protocols.[43] The adapted traffic traverses ATM core networks.

The lack of ITU-T involvement in MPLS and GMPLS may derail global adoption of protocols as network standards. Lacking ITU-T support, MPLS and GMPLS may become a North American-only technology, which will doom both protocols to failure. It will be several years before the full weight of ITU-T's decisions and the fate of MPLS and GMPLS are known.

The many developments of IP-related standards and the eventual conversion of voice services to data-centric networks portend sweeping changes within the communications infrastructure. Change creates hazards to the unprepared and opportunity for those having vision. Many services used in emergency situations will change, the underlying infrastructure will be replaced, and without careful attention, special arrangements in support of NS/EP agencies may be lost. At the same time, sweeping change opens many avenues for improvements in support of NS/EP services. The next few years represent a crossroad in communication infrastructure development. Natural emergencies, past international confrontations, and the terrorist attacks of September 11, 2001 highlight the importance of NS/EP support within our national communication infrastructure. Now is the time to seize an opportunity to improve the overall support of NS/EP traffic by making known NS/EP requirements within the IETF and the ITU-T. The fruits of such efforts could enhance NS/EP agency support within both the electronic and the optical layers of the national communication networks.

7.0 CONCLUSIONS

Two primary factors motivate the development of MPLS: rapidly growing IP-centric traffic across carrier networks, and inadequate support for IP traffic within the carrier network infrastructure. IP-centric data traffic and the conversion of telephony network to voice-over-IP is forcing carriers to reconsider their network architectures. The large installed base of SONET equipment supports telephony well, but is poorly suited to rapid provisioning of wide bandwidth data services. ATM switching equipment lacks scalable adaptation protocols necessary to provision large VPNs and carry large volumes of IP-over-ATM effectively. Consequently, carriers find themselves with serious service diseconomies that grow with the ever-increasing volume of IP traffic.

In a sense, MPLS is an evolutionary extension to ATM and its predecessor frame relay. Each evolutionary step capitalizes upon the strengths of its predecessor and adds new features addressing omissions in prior protocols. After all, the MPLS label is essentially a modified form of the ATM VCI/VPI, which in turn takes its heritage from the frame relay DLCI. The more important aspects of MPLS are its direct support of IP multipoint-to-point connections and many other IP-related features.

Developers of MPLS and GMPLS standards strive to reduce network complexity, automate service provisioning, and provide better traffic engineering. MPLS developed as an enhanced packet forwarding mechanism and improves traffic engineering mechanism for IP networks. GMPLS takes the next step beyond MPLS and becomes a general-purpose control plane for IP traffic traversing packet switched, cell switched, TDM, wavelength switched, and/or fiber switched networks.

Unlike MPLS, GMPLS is not a data transport protocol.[47] Rather, GMPLS is a control plane protocol designed to carry signaling across five different types of data planes: packet capable (IP router), layer-2 cell switching (ATM), TDM multiplexing (SONET), WDM multiplexing (wavelength), and fiber strand switching. Network components set up and tear down connections within their respective layers according to traditional methods. GMPLS uses OSPF or IS-IS to compute the route, RSVP-TE or CR-LDP to signal the LSP, and LMP to maintain the connection.

The promises of GMPLS are exciting, but must be tempered with the reality that both MPLS and GMPLS are new and developing protocols. They promise to fix many of the IP-support shortfalls within ATM. In addition, GMPLS will lead to a much higher degree of integration within the network, possibly leading to a single control plane distinctly separate from the interconnected data planes of ATM, SONET, OXC, WDM, and fiber circuit switching. GMPLS promises to be the control plane for high-speed core networks in much the same way that SS7 is the control plane for the telephony plane, which, in the case of telephony and SS7, is comprised of circuit switching systems and SONET.

If GMPLS is adopted, full unification and standardization of control plane signaling would effectively create a single network service comprised of electronic and optical data planes. Provisioning and restoration of services would be completely automatic.

Urgent consideration should be given for the importance of national security and emergency preparedness (NS/EP) within the MPLS, GMPLS, and advanced optical switching protocols. Today, IP, frame relay, and ATM offer varying degrees of prioritization for NS/EP-related data traffic ranging from none within TCP/IP protocols to significant QoS guarantees within ATM protocols. There are opportunities to improve the handling of NS/EP traffic within MPLS and GMPLS provided that the requirements to do so are included during the formative stages of the standards. Immediate action is needed to include NS/EP requirements in developing MPLS and GMPLS protocols. Attention should also be given to ASTN and ASOTN protocol developments forthcoming from the ITU-T during next few years. New protocol developments within the carrier core network offer a unique opportunity to implement special considerations for traffic critical to United State's responses to natural disasters, terrorist attacks, and acts of war.

The creation of a completely unified control plane for carrier networks is from five to ten years away, given the time to create standards and upgrade carrier-class networks. The huge installed base of network equipment creates financial inertia that must be dealt with in the context of market competition, ongoing carrier profitability, carrier staff training, and massive deployment logistics. It took a decade to deploy SONET on a wide scale. ATM is the recent arrival, having only been prevalent within the carrier networks within the last five years. It will take time for any transition to a new network technology, no matter how beneficial it may be to the carriers.

The demise of ATM will not be immediate. Carriers invested heavily in ATM equipment, training, and service support systems. Many services such as DSL and virtual private network services depend upon ATM. However, the die may be cast and within the next decade, ATM may gradually be replaced by MPLS, GMPLS, and recent developments in photonic packet switching, provided that MPLS and GMPLS are adopted by the industry.

There are many voids within the MPLS and GMPLS protocols. A number of features are yet to be defined. MPLS deployments are sparse, geographic coverage is limited when compared to ATM-based services, and there are differences in the features offered between MPLS services. GMPLS is still a protocol on the drawing board. There are no GMPLS deployments, and much of the protocol requires refinement.

The lack of international standards sanctioning by the ITU-T leaves the long-term viability of MPLS and GMPLS in doubt. MPLS and GMPLS are carrier network protocols. The protocols will see few implementations within enterprise networks for the foreseeable future. It is unlikely that the carriers will adopt either protocol on a broad scale without ITU-T codification.

For its part, the ITU-T is considering several network architectures as improvements upon the current ATM and SONET-based architecture. There is general recognition that a new architecture is needed to improve provisioning and scalability within IP-centric carrier networks. The ITU-T will take time to weigh the best technologies for a new global network architecture before it chooses the underlying protocols.

Development of MPLS and GMPLS is an unfolding story in which many chapters remain to be written. The factors that brought about MPLS and GMPLS will ultimately lead to major changes in the carrier network architecture. A derivative of MPLS and GMPLS or a derivative of ATM and SONET will surely replace the existing carrier architecture. Time will pass; standards will come and go before the final winner is left standing.

8.0 LIST OF REFERENCES

[1] Duffy, Jim. "MPLS readies networks for user boom." Network Word Fusion. November 12, 2001. <http://www.nwfusion.com/news/2001/1112mpls2.html>.

[2] Krapf, Eric. "Can Fiber Make It Down The Last Mile?" Business Communications Review. February 2000.

[3] Clavena, Scott. "Optical Signaling Systems." Light Reading, Inc. January 28, 2002. <http://www.lightreading.com/document.asp?site=lightreading&doc_id=7098&page_number=1>.

[4] Viswanathan, Aurn, Nancy Feldman, Zheng Wang, and Ross Callon. "Evolution of Multiprotocol Label Switching." IEEE Communications Magazine. May 1998.

[5] Banerjee, Ayan, John Drake, Jonathan Lang, Brad Turner, Kireeti Kompella, and Yakov Rekhter. "Generalized Multiprotocol Label Switching: An Overview of Routing and Management Enhancements." IEEE Communications Magazine. January 2001.

[6] Badran, Hosein F. "Service Provider Networking Infrastructures with MPLS." Sixth IEEE Symposium on Computers and Communications, Mammamet, Tunesia. July 3-5, 2001.

[7] Hommes, Ferdinand, Eva Pless, Lothar Zier. "Did MPOA achieve its objective?" Computer Networks, 34 (2000) 895-904, Elsevier Science B.V. 2000.

[8] McCutcheon, Mark. "Multicast Over ATM." University of British Columbia. July 2, 1997 <http://www.cs.ubc.ca/nest/dsg/tevia_files/techreport/node26.html>.

[9] Chang, Gee-Kung. "Optical Label Switching." Telcordia Technologies, Defense Advanced Research Projects Agency (DARPA) NGI PI Meeting. October 4, 2000.

[10] McCutcheon, Mark. "Other Models: SITA." University of British Columbia. July 2, 1997 <http://www.cs.ubc.ca/nest/dsg/tevia_files/techreport/node25.html>.

[11] McCutcheon, Mark. "Aggregate Route—Based IP Switching (ARIS)." University of British Columbia. July 2, 1997 <http://www.cs.ubc.ca/nest/dsg/tevia_files/techreport/node22.html>.

[12] McCutcheon, Mark. "Cell Switching Routers (CSR)," University of British Columbia. July 2, 1997 <http://www.cs.ubc.ca/nest/dsg/tevia_files/techreport/node24.html>.

[13] McCutcheon, Mark. "Ipsilon IP Switch," University of British Columbia. July 2, 1997 <http://www.cs.ubc.ca/nest/dsg/tevia_files/techreport/node23.html>.

[14] McCutcheon, Mark. "Tag Switching," University of British Columbia. July 2, 1997 <http://www.cs.ubc.ca/nest/dsg/tevia_files/techreport/node21.html>.

[15] "The MPLS FAQ." The MPLS Resource Center. January 10, 2002 <http://www.mplsrc.com/faq1.shtml>.

[16] Kocialski, Cynthia. “A Primer on MPLS From Label to Lambda Switching.” Vesta Corporation, Santa Clara, California. May 2000 <info@vesta-corp.com>.

[17] Gallaher, Rick. “An Introduction to MPLS.” January 10, 2002 <http://www.convergedigest.com/Bandwidth/archive/010910TUTORIAL-rgallaher1.htm>.

[18] “Encoding MPLS Labels.” January 21, 2002 <http://www.riverstonenet.com/support/mpls/encoding_mpls_labels.htm>.

[19] Awduche, Daniel O., Alan Hannan, and XiPeng Xiao. “Applicability Statement for Extensions to RSVP for LSP-Tunnels.” Network Working Group, p. 2. December 2001 <http://www.ietf.org/rfc/rfc3210.txt?number=3210>.

[20] Brittain, Paul and Adrian Farrel. “MPLS Traffic Engineering: A Choice of Signaling Protocols.” Data Connection Limited, pp. 4-5, 8-13, 20. January 17, 2000.

[21] Chen, Thomas M. and Willie Wu. “Multi-protocol lambda switching for IP over optical networks.” Proceedings of SPIE – the International Society for Optical Engineering, Vol. 4211, pp. 165-172. November 6-7, 2000.

[22] Ragsdale, Gary L., Myron L. Moodie, Scott J. Schneider, and Ryan D. Lamm. “Internet2: Its Architecture, Goals, and Opportunities,” p. 19. Technical Information Bulletin 01-XX to NCS. Southwest Research Institute Project 10.03607. April 2001.

[23] “Traffic Engineering With Multiprotocol Label Switching,” pp. 3, 12-20, 25-27. Avici Systems Inc. March 16, 2000.

[24] Gallaher, Rick. “Introduction to MPLS Label Distribution and Signaling.” Converge! Network Digest. November 1, 2001 <http://www.convergedigest.com/tutorials/mpls2/page1.htm>.

[25] Duffy, Jim. “MPLS lays foundation for new VPN services.” Network Word Fusion. November 19, 2001 <http://www.nwfusion.com/news/2001/1119mpls3.html>.

[26] Masud, Sam. “MPLS Branches Out,” p. 3. Telecommunications Online. September 2001.

[27] Marsan, Carolyn Duffy. “Experts call MPLS bad for ‘Net,’” pp. 1-3. Network World Fusion. August 6, 2001 <http://www.nwfusion.com/news/2001/0806mpls.html>.

[28] Evans, John. “MPL(ambda)S & Generalized MPLS: An Overview.” Cisco Systems. February 1, 2002 <joevans@cisco.com>, <http://www.ripe.net/ripe/meetings/archive/ripe-39/presentations/mpls-overview/sld001.html>.

[29] “A GMPLS Taxonomy,” pp. 1-3. Light Reading – The Global Site For Optical Networking. January 8, 2002. <http://www.lightreading.com/document.asp?doc_id=7098&page_number=6>.

[30] Banerjee, Ayan, John Drake, Jonathan Lang, Brad Turner, Daniel Awduche, Lou Berger, Kireeti Kompella, and Yakov Rekhter. “Generalized Multiprotocol Label Switching: An Overview of Signaling Enhancements and Recovery Techniques.” IEEE Communications Magazine. July 2001.

[31] Ragsdale, Gary L., Myron L. Moodie, and Ryan D. Lamm. "Photonic Network Architecture: Next Generation Internet Applications." Technical Information Bulletin 01-2 to NCS. Southwest Research Institute Project 10.03607. July 2001.

[32] "Our Latest Thinking," p. 6. Telcordia – Our Latest Thinking. February 7, 2002 <http://www.telcordia.com/research/thinking.html>.

[33] Khanzode, Rutuja. "Optical Packet Switching." http://research.umbc.edu/~ychen/ee635/OPTICAL_PACKET_SWITCHING_Rutuja_Khanzode.pdf>.

[34] Greenfield, David. "Global MPLS Services? Not So Fast!" Network Magazine. February 2002 <www.networkmagazine.com>.

[35] Duffy, Jim. "MPLS facing slow adoption, despite flurry of market hype – Part 1." Network Word Fusion. November 5, 2001 <http://www.nwfusion.com/news/2001/1105mpls.html>.

[36] Kang, Sun-Moo, Young-Il, Choi, and Byeong-Nam Yoon. "IP/ATM Integration, Issues, Activities, and Suggestions." 1999 Internet Workshop, IEEE, Osaka, Japan, 1999.

[37] McCutcheon, Mark. "Integrated—PNNI (I—PNNI)." University of British Columbia. July 2, 1997 <http://www.cs.ubc.ca/nest/dsg/tevia_files/techreport/node18.html>.

[38] Matsumoto, Craig and Loring Wirbel, "Network OEMs stick with SONET, ATM attack." EE Times. January 28, 2002 <http://www.eetimes.com/story/OEG20020128S0039>.

[39] Gimpelson, Terri. "Carriers: New services can wait." Network World. March 18, 2002 <http://www.nwfusion.com/news/2002/0318carriers.html>.

[40] Schoen, John W. "A telecom hangover … that won't go away. " MSNBC. March 15, 2002 <http://www.msnbc.com/news/720244.asp?0si=->.

[41] Wirbel, Loring. "40-Gbit technology arrives in search of a market." EE Times. March 15, 2002 <http://www.eetimes.com/story/OEG20020315S0061>.

[42] Wirbel, Loring. "CableLabs regroups for residential platform push." EE Times. March 18, 2002 <http://www.eetimes.com/story/OEG20020318S0021>.

[43] McLeod, Stuart. *ATM Internetworking – Revision 5.0*. Global Knowledge, Inc., 1999.

[44] Cheng, Dean and Robert Haim. "Challenges roil MPLS and GMPLS." EE Times. October 18, 2001 <http://www.planetanalog.com/story/OEG20011018S0027>.

[45] Lee, Ryan. "IGP Routing: OSPF and Integrated IS-IS." SpirentCom.Com, 2nd Quarter 2001.

[46] "ATM and MPLS Forums to Collaborate on Internetworking Standard." Converge! Network Digest. January 17, 2002 <http://www.convergedigest.com/standards/ standardsarctile.asp?ID=2238>.

[47] Greenfield, David. “Optical Standards: A Blueprint for the Future.” Network Magazine. October 2001.

[48] Whittington, Brad. “The Current State of Optical Signaling Specifications.” SpirentCom.Com. 2nd Quarter 2001.