Generalized Multiprotocol Label Switching (GMPLS)

Definition and Overview

The premise of multiprotocol label switching (MPLS) is to speed up packet forwarding and provide for traffic engineering in Internet protocol (IP) networks. To accomplish this, the connectionless operation of IP networks becomes more like a connection-oriented network where the path between the source and the destination is precalculated based on user specifics. To speed up the forwarding scheme, an MPLS device uses labels rather than address matching to determine the next hop for a received packet. To provide traffic engineering, tables are used that represent the levels of quality of service (QoS) that the network can support. The tables and the labels are used together to establish an end-to-end path called a label switched path (LSP). Traditional IP routing protocols (e.g., open shortest path first [OSPF] and intermediate system to intermediate system [IS–IS]) and extensions to existing signaling protocols (e.g., resource reservation protocol [RSVP] and constraint-based routing–label distribution protocol [CR–LDP]) comprise the suite of MPLS protocols.

Generalized MPLS (GMPLS) extends MPLS to provide the control plane (signaling and routing) for devices that switch in any of these domains: packet, time, wavelength, and fiber. This common control plane promises to simplify network operation and management by automating end-to-end provisioning of connections, managing network resources, and providing the level of QoS that is expected in the new, sophisticated applications.

This tutorial focuses on the issues that GMPLS resolves in providing a common control plane to operate across dissimilar network types (e.g., packet, time division multiplexing [TDM], and optical). Initially, a brief overview of MPLS and its evolution to GMPLS is given. Next, a summary of GMPLS protocols and important extensions is presented. In-depth coverage of the issues is then provided. At the end, some of the current outstanding issues in GMPLS are explored.

Topics

1. Introduction
2. Evolution from MPLS
3. GMPLS Issues and their Resolutions
4. GMPLS Outstanding Issues

Self-Test

Correct Answers

Glossary

1. Introduction

The emergence of optical transport systems has dramatically increased the raw capacity of optical networks and has enabled a slew of new, sophisticated applications. For example, network-based storage, bandwidth leasing, data mirroring, add/drop multiplexing [ADM], dense wavelength division multiplexing [DWDM], optical cross-connect [OXC], photonic cross-connect [PXC], and multiservice switching platforms are some of the devices that may make up an optical network and are expected to be the main carriers for the growth in data traffic.

The diversity and complexity in managing these devices have been the main driving factors in the evolution and enhancement of the MPLS suite of protocols to provide control for not only packet-based domains, but also time, wavelength, and space domains. GMPLS further extends the suite of IP-based protocols that manage and control the establishment and release of label switched paths (LSP) that traverse any combination of packet, TDM, and optical networks.

An important economic impact of GMPLS is providing the ability to automate network resource management and the service provisioning of end-to-end traffic-engineered paths. Service provisioning has been a manual, lengthy, and costly process—e.g., synchronous optical network (SONET)–based ring networks. To manually provision an end-to-end high-speed connection, a carrier must determine which SONET rings the connection traverses and provision bandwidth on each ring manually. If any ring is at full capacity, the carrier must find an alternative ring path or upgrade the capacity of a ring and propagate the information to all sites manually. These are very time-consuming processes and can take months. The deployment of GMPLS–based nodes allows carriers to automate the provisioning and management of the network and promises to

lower the cost of operation by several orders of magnitude (days or even minutes instead of weeks or months).

2. Evolution from MPLS

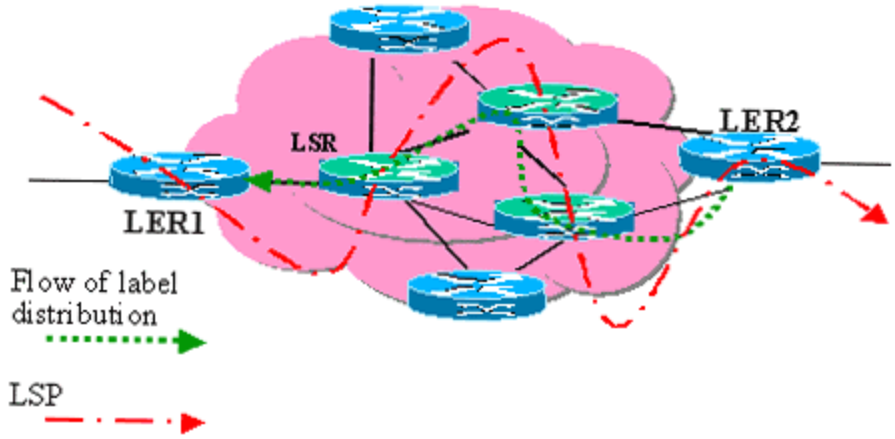
MPLS Background and Operation

MPLS extended the suite of IP protocols to expedite the forwarding scheme used by IP routers. Routers, to date, have used complex and time-consuming route lookups and address matching schemes to determine the next hop for a received packet, primarily by examining the destination address in the header of the packet. MPLS has greatly simplified this operation by basing the forwarding decision on a simple label. Another major feature of MPLS is its ability to place IP traffic on a defined path through the network. This capability was not previously possible with IP traffic. In this way, MPLS provides bandwidth guarantees and other differentiated service features for a specific user application (or flow). Current IP–based MPLS networks are capable of providing advanced services such as bandwidth-based guaranteed service, priority-based bandwidth allocation, and preemption services.

For each specific service a table of forwarding equivalence class (FEC) is created to represent a group of flows with the same traffic-engineering requirements. A specific label is then bound to an FEC. At the ingress of an MPLS network, incoming IP packets are examined and assigned a "label" by a label edge router (LER). The labeled packets are then forwarded along an LSP, where each label-switched router (LSR) makes a switching decision based on the packet's label field. An LSR does not need to examine the IP headers of the packets to find an output port (next hop). An LSR simply strips off the existing label and applies a new label for the next hop. The label information base (LIB) provides an outgoing label (to be inserted into the packet) and an outgoing interface (based on an incoming label on an incoming interface).

Signaling to establish a traffic-engineered LSP is done using a label distribution protocol that runs on every MPLS node. There are a number of different label-distribution protocols. The two most popular RSVP–traffic engineering (RSVP–TE) and CR–LDP. RSVP–TE is an extended version of the original RSVP to piggyback and distribute labels on its messages and to provide traffic-engineering capability. CR–LDP was designed specifically for this purpose. *Figure 1* shows the flow of label distribution that is carried out by the downstream LER (in this case LER2) while the LSP flow is the reverse.

Figure 1. Figure 1: An MPLS-Based Network



The MPLS framework includes extensions to existing IP link-state routing protocols. These protocols provide real-time coordination of the current network topology, including attributes of each link. MPLS extensions to OSPF and IS–IS allow nodes to not only exchange information about the network topology, but also resource information and even policy information—for example, IP addresses, available bandwidth, and load-balancing policies. Constraint-based routing algorithms use this information to compute the optimal paths for the LSPs through the network and allow complex traffic-engineering decisions to be made automatically when selecting routes through the network.

MPLS Evolution to GMPLS

Within the past year, the International Engineering Task Force (IETF) has extended the MPLS suite of protocols to include devices that switch in time, wavelength, (e.g., DWDM) and space domains (e.g., OXC) via GMPLS. This allows GMPLS–based networks to find and provision an optimal path based on user traffic requirements for a flow that potentially starts on an IP network, is then transported by SONET, and then is switched through a specific wavelength on a specific physical fiber. *Table 1* gives a summary of the GMPLS framework.

Table 1. GMPLS Framework

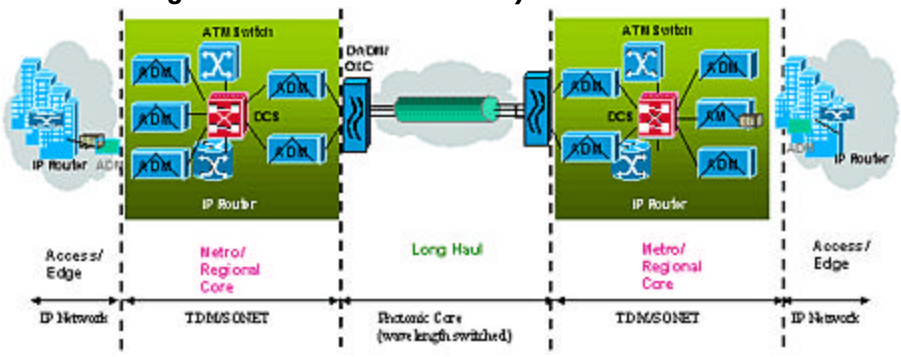
Switching Domain	Traffic Type	Forwarding Scheme	Example of Device	Nomenclature
Packet, cell	IP, asynchronous transfer mode (ATM)	Label as shim header, virtual channel connection (VCC)	IP router, ATM switch	Packet switch capable (PSC)

Time	TDM / SONET	Time slot in repeating cycle	Digital cross-connect system (DCS), ADM	TDM capable
Wavelength	Transparent	Lambda	DWDM	Lambda switch capable (LSC)
Physical space	Transparent	Fiber, line	OXC	Fiber switch capable (FSC)

The basic challenge for an all-encompassing control protocol is the establishment, maintenance, and management of traffic-engineered paths to allow the data plane to efficiently transport user data from the source to the destination. A user flow starting from its source is likely to travel several network spans–for example, an access or edge network that aggregates the flows from multiple users (e.g., enterprise applications) to feed into a metro network that is SONET–based or ATM–based that itself aggregates multiple flows from various edge networks to feed into a long-haul network that uses lambdas to transport the aggregated flow of multiple metro networks. The reverse path is used to deliver data to its destination.

These networks and the typical devices used are shown in *Figure 2*.

Figure 2. Dissimilar Networks That Carry End-User Traffic (Click on image for full-size version.)



Summary of the GMPLS Protocol Suite

The evolution of MPLS into GMPLS has extended the signaling (RSVP–TE, CR–LDP) and routing protocols (OSPF–TE, IS–IS–TE). The extensions accommodate the characteristics of TDM / SONET and optical networks.

A new protocol, link-management protocol (LMP), has been introduced to manage and maintain the health of the control and data planes between two neighboring nodes. LMP is an IP-based protocol that includes extensions to RSVP–TE and CR–LDP.

Table 2 summarizes these protocols and the extensions for GMPLS.

Table 1. GMPLS Protocols

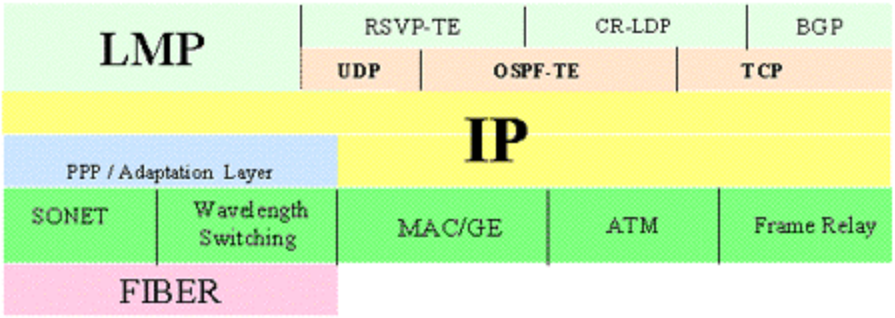
Protocols		Description
Routing	OSPF–TE, IS–IS–TE	Routing protocols for the auto-discovery of network topology, advertise resource availability (e.g., bandwidth or protection type). The major enhancements are as follows: Advertising of link-protection type (1+1, 1:1, unprotected, extra traffic) Implementing derived links (forwarding adjacency) for improved scalability Accepting and advertising links with no IP address—link ID Incoming and outgoing interface ID Route discovery for back-up that is different from the primary path (shared-risk link group)
Signaling	RSVP–TE, CR–LDP	Signaling protocols for the establishment of traffic-engineered LSPs. The major enhancements are as follows: Label exchange to include non-packet networks (generalized labels) Establishment of bidirectional LSPs Signaling for the establishment of a back-up path (protection Information) Expediting label assignment via suggested label Waveband switching support—set of contiguous wavelengths switched together
Link Management	LMP	**Control-Channel Management:** Established by negotiating link parameters (e.g., frequency in sending keep-alive messages) and ensuring the health of a link (hello protocol) **Link-Connectivity Verification:** Ensures the physical connectivity of the link between the neighboring nodes using a PING–like test message

		Link-Property Correlation: Identification of the link properties of the adjacent nodes (e.g., protection mechanism) **Fault Isolation:** Isolates a single or multiple faults in the optical domain

The details of each protocol and their enhancements are found in the references at the end of this tutorial.

The protocol stack is shown in *Figure 3*.

Figure 3. The GMPLS Protocol Stack



Note that the IS–IS–TE routing protocol stack is similar to OSPF–TE with the exception that, instead of IP, connectionless network protocol (CLNP) is used to carry IS–IS–TE's information.

3. GMPLS Issues and Their Resolutions

For a control plane to be used for all of these dissimilar networks types, the following issues must be considered:

1. Data forwarding is now not limited to that of merely packet forwarding. The general solution must be able to retain the simplicity of forwarding using a label for a variety of devices that switch in time or wavelength, or space (physical ports).

2. Not every type of network is capable of looking into the contents of the received data and of extracting a label. For instance, packet networks are able to parse the headers of the packets, check the label, and carry out decisions for the output interface (forwarding path) that they have to use. This is not the case for TDM or optical networks. The equipments in these

types of networks are not designed to have the ability to examine the content of the data that is fed into them.

3. Unlike packet networks, in TDM, LSC, and FSC interfaces, bandwidth allocation for an LSP can be performed only in discrete units. For example, a packet-based network may have flows of 1 Mbps to 10 or 100 Mbps. However, an optical network will use links that have fixed bandwidths: optical carrier (OC)–3, OC–12, OC–48, etc. When a 10 Mbps LSP is initiated by a PSC device and must be carried by optical connections with fixed bandwidths—e.g., an OC–12 line—it would not make sense to allocate an entire 622M line for a 10M flow.

4. Scalability is an important issue in designing large networks to accommodate changes in the network quickly and gracefully. The resources that must be managed in a TDM or optical network are expected to be much larger in scope than in a packet-based network. For optical networks, it is expected that hundreds to thousands of wavelengths (lambdas) will be transporting user data on hundreds of fibers.

5. Configuring the switching fabric in electronic or optical switches may be a time-consuming process. For instance, in a DCS that is capable of switching tens of thousands of digital signal (DS)–1 physical ports, identifying the connection between the input/output ports could be time consuming as fewer ports become available to accommodate incoming user traffic. Latency in setting up an LSP within these types of networks could have a cumulative delaying effect in setting up an end-to-end flow.

6. SONET networks have the inherent ability to perform a fast switchover from a failed path to a working one (50 milliseconds). GMPLS' control plane must be able to accommodate this and other levels of protection granularity. It also needs to provide restoration of failed paths via static (pre-allocated) or dynamic reroute, depending on the required class of service (CoS).

These issues are summarized in *Table 3* and discussed in subsequent sections in more detail.

Table 3. Summary of Issues in a Common Control-Plane Approach

Issue	GMPLS Solution(s)	Protocol(s)	Notes
Switching	Generalized label	Signaling: RSVP–TE,	LSP to start and end on

diversity		CR–LDP	the same type of device
Forwarding diversity	Logical or physical separation of control and data	All	Signaling and routing to travel out of band
Configuration	Suggested label Bidirectional LSPs	Signaling	Expedite LSP set-up
Scalability	Forwarding adjacency Link bundling Hierarchical LSPs	Routing and signaling: OSPF–TE, IS–IS–TE	Lower link database size Bandwidth scalability
Reliability	Protection and restoration (M:N, 1+1) Shared-risk link group for path diversity	LMP Routing: OSPF–TE, IS–IS–TE	Simulate SONET bidirectional line-switched ring (BLSR), unidirectional path-switched ring (UPSR) User disjoint route for back-up
Efficient use of network resources	Hierarchical LSP Unnumbered links	Signaling / routing	Save on excess use of scarce IP addresses

Switching Diversity

Generalized Label and Its Distribution

To be able to support devices that switch in different domains, GMPLS introduces new additions to the format of the labels. The new label format is referred to as a "generalized label" that contains information to allow the receiving device to program its switch and forward data regardless of its construction (packet, TDM, lambda, etc.). A generalized label can represent a single wavelength, a single fiber, or a single time-slot. Traditional MPLS labels—e.g., ATM, VCC, or IP shim—are also included. The information that is embedded in a generalized label includes the following:

1. LSP encoding type that indicates what type of label is being carried (e.g., packet, lambda, SONET, etc.)

2. Switching type that indicates whether the node is capable of switching packets, time-slot, wavelength, or fiber

3. A general payload identifier to indicate what payload is being carried by the LSP (e.g., virtual tributary [VT], DS-3, ATM, Ethernet, etc.)

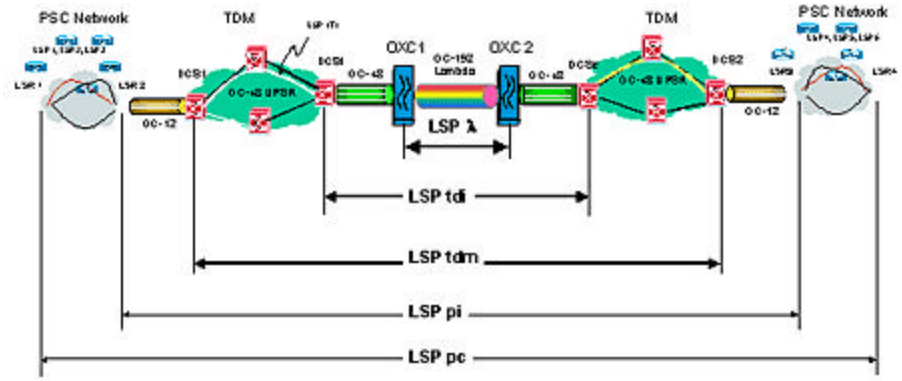
Details of a GMPLS label can be found in reference [2].

Similar to MPLS, label distribution starts from the upstream LSR requesting a label from the downstream LSR. GMPLS takes this further by allowing the upstream LSR to suggest a label for a LSP that can be overridden by the downstream LSR. (Suggested labels are covered in a later section.)

LSP Creation in GMPLS-Based Networks

Establishing an LSP in a GMPLS network is similar to that of MPLS networks. Figure 4 shows a packet network (PSC) connected via an OC–12 pipe to DCS1 in the upper TDM network. Both of the TDM networks shown use a SONET UPSR OC–48 ring architecture. The two TDM networks are connected via two OXCs capable of delivering multiple OC–192 lambdas. The goal is to establish an LSP (LSPpc) between LSR1 and LSR4.

Figure 4. Establishing an LSP through Heterogeneous Networks with GMPLS



To establish the LSPpc between LSR1 and LSR4, other LSPs in the other networks must be established to tunnel the LSPs in the lower hierarchy. For example, per *Figure 4*, LSP1T1 will carry LSP1, LSP2, and LSP3 if the sum of the traffic-engineering requirements of the packet LSPs can be accommodated by it.

This is done by sending a PATH / Label Request message downstream to the destination that will carry the lower hierarchy LSP. For example, DSCi sends this message to OXC1, destined for DSCe. When received by OXC1, it will then create

an LSP between it and OXC2. Only when this LSP (LSPl) is established will an LSP between DSCi to DSCe be established (LSPtdi).

The PATH / Label Request message contains a Generalized Label Request with the type of LSP (i.e., the layer concerned), and its payload type (e.g., DS–3, VT, etc.). Specific parameters—such as type of signal, local protection, bidirectional LSP, and suggested labels—are all specified in this message. The downstream node will send back a RESV / Label Mapping message including one generalized label that may contain several generalized labels.

When the generalized label is received by the initiator LSR, it can then establish an LSP with its peer via RSVP / PATH messages per network domain. In Figure 4, the following sequence has taken place:

1. LSP is established between OXC1 and OXC2 (LSPl) and capable of delivering OC–192 wavelength to tunnel in TDM LSPs.

2. LSP is established between DSCi and DSCe (LSPtdi).

3. LSP is established between DS–1 and DS–2 (internal LSPs within the two TDM networks are established prior to the establishment of this LSP).

4. LSP is established between LSR2 and LSR3 (LSPpi).

5. LSPpc is established between LSR1 and LSR4.

Forwarding Diversity

MPLS devices are capable of discerning the contents-of-information unit that is passed between them—e.g., a packet or a cell that has header information. They need to examine the label (e.g., shim header) to determine the output port and the output label for an incoming packet. The label-swapping paradigm logically separates the data and the control planes.

GMPLS extends this paradigm to those devices that are designed to lookup any headers when they receive the user data. In this case, GMPLS allows the data plane and the control plane to be physically, or logically, separate. For example, the control path between two devices could travel an external line such as an Ethernet connection, or other types of physical links. GMPLS does not mandate how the control information is to be transported between two nodes.

The selection of a medium to carry the control information between the two GMPLS nodes can impact the economics of the network operator. Clearly, a

single fiber should not be used to carry this information between two geographically separate devices—e.g., two DCSes in a SONET ring network. Other connection types may be costly to use—e.g., an X.25 connection. One approach is to take a logical slice of a line—e.g., synchronous transport signal (STS)–1—and use the data communication channel (DCC) bytes in the SONET overhead to carry the control information. These bytes are comprised of section and line overhead (three and nine bytes, respectively) and can both be used for this purpose. Together they provide a 768 kbps channel for the exchange of control messages. They can be used in each direction between two adjacent nodes. This is a highly efficient method that does not take away bandwidth that could be used for user data traffic.

Configuration

When an LSP is being established starting from the access network, it may require the establishment of several other LSPs along its end-to-end path. These intermediate LSPs may be established on TDM– and/or LSC–based devices. These devices have different internal characteristics, and, therefore, GMPLS must accommodate these differentials in such a way as to expedite the establishment of the end-to-end LSPs. Two important new concepts that are introduced in GMPLS to address these differences are as follows.

Suggested Label

As mentioned in an earlier section, an upstream node can optionally suggest a label to its downstream node. The downstream node has the right of refusal and may propose its own. Nevertheless, this operation is crucial to systems that require time-consuming processes to configure their switch fabric—for example, a DCS with high switching granularity (e.g., DS–1, DS–3) and thousands of ports that must go through a time-consuming operation in configuring its switching fabric. Recall that a label in this case is used to quickly find the internal path between an input and an output port. A suggested label allows the DCS to configure itself with the proposed label, instead of waiting to receive a label from the downstream node, and then configure its hardware. Suggested labels are also important in expediting the set-up of back-up paths (LSPs) for a failed LSP. However, if the downstream device rejects the suggested label and offers its own, the upstream device must re-configure itself with the new label.

Bidirectional LSP

Network protection—e.g., against fiber cuts—in optical networks is provided with back-up fibers, such as four-wire BLSR or two-wire BLSR architectures. Similarly, LSPs in an optical network need to be protected. This is accomplished by establishing two unidirectional LSPs—one LSP to protect the other. Bidirectional LSPs must have the same traffic-engineering and restoration requirements.

GMPLS supports the setup of bidirectional LSPs via one set of signaling protocol messages (e.g., RSVP/PATH and RESV). This helps to avoid the extraneous exchange of control messages, race conditions, additional route look-ups, and configuration-latency in setting up the internal input/output (I/O) paths in an optical switch.

Scalability

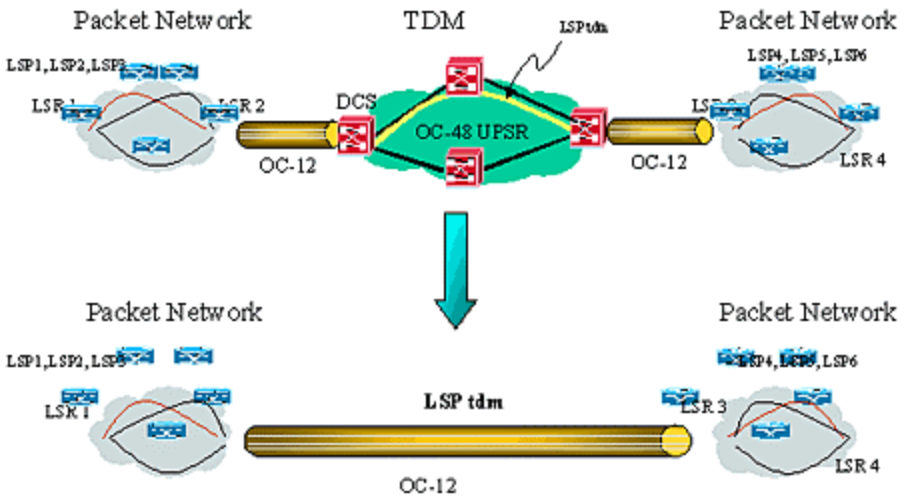
Forwarding Adjacency–LSP (FA–LSP)

A FA–LSP is a GMPLS–based LSP to carry other LSPs. An FA–LSP established between two GMPLS nodes can be viewed as a virtual link with its own traffic-engineering characteristics and can be advertised into the OSPF/IS–IS as a normal link like any other physical link. An FA–LSP may be incorporated into the link-state database and used in routing-path calculation to carry other LSPs. This can reduce the size of the database, and, consequently, the time that is spent in the table look-up operation.

An FA–LSP may be either a numbered or unnumbered and may be bundled with other links, whether they are FA–LSPs or normal links. Both concepts are discussed in later sections.

Figure 5 shows how a TDM LSP (LSPtdm) can be viewed as a link that connects two packet-based networks. This LSP can be viewed as a single link in the packet-based LSRs of the two PSC networks, instead of all of the physical links in the TDM network.

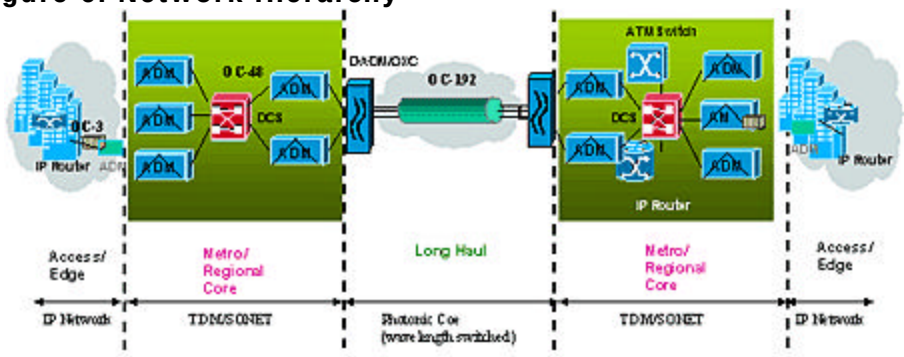
Figure 5. Forwarding Adjacency



Hierarchical LSP

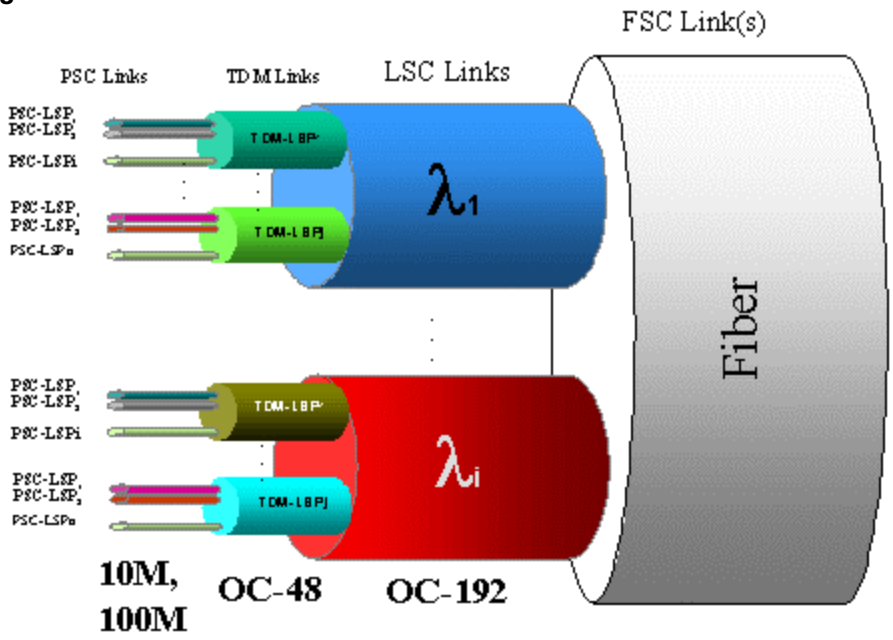
The network hierarchy (access, metro, and long haul) shown in *Figure 6* provides an increasing bandwidth capacity per hierarchy. When an end-to-end flow is to be establish for a particular enterprise application, that flow will traverse networks that use devices that may not be designed to configure connections with flexible bandwidth levels—i.e., only discrete bandwidth are available. In this case, a single OC–192 physical link between two optical switches should not be expected to carry a traffic that is only 100M or even 2.5G, as it would be wasteful and highly inefficient. It is better to aggregate lower-speed flows into higher-speed ones. This brings the notion of hierarchical LSP.

Figure 6. Network Hierarchy



A natural hierarchy is established wherein a group of PSC–LSPs are nested within TDM–LSPs that are then nested within a LSC that is part of a group of LSCs within an FSC. The link multiplex capability parameter introduced in GMPLS specifies this ordering when an LSP is being established. Clearly, bandwidth that remains within each LSP can and should be used to accept and include additional LSPs from lower-hierarchy LSPs. *Figure 7* shows this hierarchy.

Figure 7. Hierarchical LSPs



Link Bundling

It is expected that an optical network will deploy tens to hundreds of parallel fibers, each carrying hundreds to thousands of lambdas between two nodes. To

avoid a large size for the link database and provide better scaling of the network, GMPLS has introduced the concept of link bundling.

Link bundling allows the mapping of several links into one and advertising that into the routing protocol—i.e., OSPF, IS–IS. Although, with the increased level of abstraction, some information is lost, this method greatly lowers the size of the link-state database and the number of links that need to be advertised. A bundled link needs only one control channel, which further helps to reduce the number of messages exchanged in signaling and routing protocols.

GMPLS flexibly allows the bundling of both point-to-point (PTP) links and LSPs that were advertised as links to OSPF (forward adjacency).

There are restrictions in bundling links. These are as follows:

1. All links that comprise a bundled link must begin and end on the same pair of LSRs.

2. All links that comprise a bundled link must be of the same link type (e.g., PTP or multicast).

3. All links that comprise a bundled link must have the same traffic metric (e.g., protection type or bandwidth).

4. All links that comprise a bundled link must have the same switching capability—PSC, TDMC, LSC, or FSC.

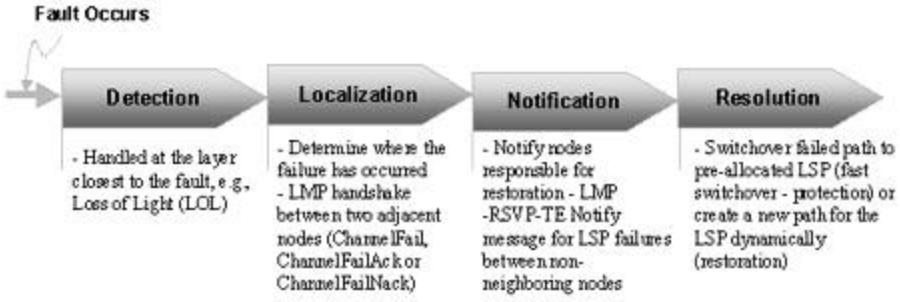
Bundled links result in loss of granularity in the network resources. Nevertheless, the gain in the reduction of link-state database entries and the speed gain in table look-ups far outweigh the lost information.

Reliability

A key attribute of GMPLS suite of protocols is the ability to enable automated fault management in network operation. A fault in one type of the network must be isolated and resolved separately from other networks. This is a very important feature for end-to-end LSPs that are tunneled in other LSPs that require higher degrees of reliability along the hierarchy. A common control plane that spans dissimilar networks must be able to address the varying degrees of reliability requirements within each network span.

The steps that are necessary to carry out fault management are shown in *Figure 8*.

Figure 8. Fault-Management Process in GMPLS

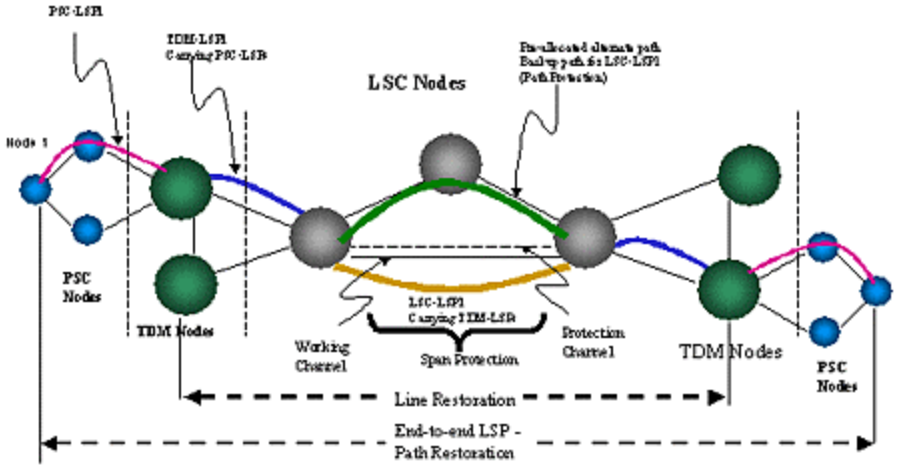


GMPLS provides protection against failed channels (or links) between two adjacent nodes (*span protection*) and end-to-end protection (*path protection*). The OSPF and IS–IS extensions for GMPLS advertise the link-protection-type parameter to include span protection while the route is being computed. After the route is computed, signaling to establish the backup paths is carried out via RSVP–TE or CR–LDP. For span protection, 1+1 or M:N protection schemes are provided by establishing secondary paths through the network and using signaling messages to switch from the failed primary path to the secondary path. *Figure 9* depicts span and path protections.

For end-to-end path protections, the primary and secondary paths are computed and signaled to indicate that the two paths share reservations. Shared-risk link group is an optional mechanism that allows the establishing of back-up LSPs that do not have any links in common with the primary LSP. This is achieved in the routing extension of OSPF / IS–IS.

The restoration of a failed path refers to the dynamic establishment of a back-up path. This process requires the dynamic allocation of resources and route calculation. Two different restoration methods are given: line and path. Line restoration finds an alternate route at an intermediate node. Path restoration is initiated at the source node to route around a failed path anywhere within the path for the specific LSP. In *Figure 9*, node 1 can initiate this new path. In general, restoration schemes take longer to switch to the back-up path, but they are more efficient in bandwidth usage, as they do not pre-allocate any resource for an LSP.

Figure 9. Protection Schemes Supported in GMPLS



Efficient Resource Usage

The inclusion and management of resources in TDM and optical devices, via an IP-based control plane, requires new levels of optimization. Link bundling was discussed earlier as a method to reduce the size of the link-state database per TDM and optical networks. Another major issue in TDM and optical networks is their potential usage of IP addresses. This is discussed next.

Unnumbered Links

Instead of assigning a different IP address to each TDM or optical link, the concept of "unnumbered links" is used to keep track of these types of links. This is necessary because of the following:

1. The number of TDM channels, wavelengths, and fibers can easily reach a point where their management, per IP address, will become very time-consuming.

2. IP addresses are considered scarce resources.

An unnumbered link is a link that has no IP address—instead, a combination of a unique router ID and link number is used to represent it. These links carry traffic-engineering information and can be specified in the signaling plane, just like a regular link with an IP address.

RSVP–TE and CR–LDP have both been extended to carry this information in the signaling plane. The same has been done in the routing protocols (OSPF–TE, IS–IS–TE). For further information see references [4,5].

4. GMPLS Outstanding Issues

The GMPLS suite of protocols (extensions) is not fully standardized as of this writing. It is expected that they will soon become so. In the meantime, there are several unresolved issues that deserve attention. These are briefly discussed next.

Security

Traditional IP routing examines the contents of the header of a received packet to determine the next hop for it. While time-consuming, this step allows the establishment of firewalls, as the necessary information is available in the packet header—e.g., the source and the destination addresses that are globally unique. In contrast, GMPLS/MPLS labels are used to speed up the forwarding scheme and only have local significance—i.e., the label is only understood and used internally by the GMPLS device itself. As such, these labels cannot be used for access-control or network-security purposes. One way to establish security in a GMPLS network is to enforce access security during the connection set-up time, like other connection-oriented networks—e.g., X.25 or ATM.

Interworking

The success of GMPLS will partially depend on its ability to communicate with the many existing ATM or Frame Relay network infrastructures. Interworking with ATM and Frame Relay networks will allow transport of control and data plane information exchanged between two similar networks (e.g., two ATM networks) through a dissimilar network (e.g., GMPLS).

The implementation of interworking functions between these networks face these issues:

1. Interworking in the control plane is very complicated as different suites of protocols are used in each network (e.g., routing, private network-to-network interface [PNNI] in ATM versus OSPF–TE in GMPLS networks).

2. The maintenance of end-to-end service quality as usage data travels through dissimilar network types is essential.

3. GMPLS switching can be packet-based, TDM–based, wavelength-based, waveband-based, or fiber-based. This creates quite a few combinations in the data-plane interworking context between GMPLS networks and ATM or frame-relay (FR) networks, which carry data in cells or frames, respectively.

Several industry forums are currently addressing the specifics of interworking between these networks (e.g., the MPLS Forum, the ATM Forum, the Frame Relay Forum). Practical solutions must satisfy the carriers that manage both MPLS networks and legacy networks. These solutions remain undefined at this time.

Network Equilibrium

When a new resource is deleted or added in a GMPLS network, the set of control information that is exchanged is larger than that of a traditional IP network. GMPLS uses traffic-engineering models that include introducing a set of traffic parameters, associated with data links, performing constraints-based routing, LMPs, etc. While not tested, theoretically, an MPLS/GMPLS network would take a relatively longer time to achieve an equilibrium state than would a traditional IP network when the network is disrupted.

Network-Management Systems

The most important parameter in managing a traditional IP network—e.g., the Internet—is address reachability. In contrast, the GMPLS network-management system needs to keep track of several thousands (even millions) of LSPs for their operational status, routing paths, traffic engineering, etc. This renders the GMPLS network-management system more complex relative to the management of the traditional Internet.

Self-Test

1. The control plane specified for GMPLS supports which of the following network types?

   a. Packet

   b. TDM/SONET

c. Optical

d. All of the above

2. The control plane can be physically separate from the data plane in GMPLS networks.

    a. True

    b. False

3. The LMP requires which protocol to transport its messages?

    a. IP

    b. TCP

    c. UDP

    d. CLNP

4. Forwarding adjacency allows an LSP to be reported and treated as any other link in an OSPF–TE link database.

    a. True

    b. False

5. Link bundling can be performed on which of the following?

    a. Physical links only

    b. LSPs only

    c. Both a and b

    d. Neither a nor b

6. GMPLS does not allow the upstream node to provide a label for an LSP.

    a. True

b. False

7. A GMPLS LSP can start on an IP router and end on a TDM DCS.

   a. True

   b. False

8. What type of protection is supported in GMPLS?

   a. End-to-end

   b. Spam

   c. Both a and b

   d. Neither a nor b

9. Which GMPLS concept helps with addressing the latency in the switch-fabric configuration of optical networks?

   a. Heirarchical LSPs

   b. Link bundling

   c. Suggested label

   d. All of the above

10. Each LSP in a bidirectional LSP may have different bandwidth capacities.

    a. True

    b. False

11. Which protocol is designed to localize faults in GMPLS networks?

    a. RSVP–TE

    b. OSPF–TE

c. LMP

d. Transmission control protocol (TCP)

Correct Answers

1. The control plane specified for GMPLS supports which of the following network types?

    a. Packet

    b. TDM/SONET

    c. Optical

    d. All of the above

See Topic 1

2. The control plane can be physically separate from the data plane in GMPLS networks.

    a. True

    b. False

See Topic 3

3. The LMP requires which protocol to transport its messages?

    a. IP

    b. TCP

    c. UDP

    d. CLNP

See Topic 3

4. Forwarding adjacency allows an LSP to be reported and treated as any other link in an OSPF–TE link database.

    a. True

b. False

See Topic 3

5. Link bundling can be performed on which of the following?

   a. Physical links only

   b. LSPs only

   c. Both a and b

   d. Neither a nor b

See Topic 3

6. GMPLS does not allow the upstream node to provide a label for an LSP.

   a. True

   b. False

See Topic 3

7. A GMPLS LSP can start on an IP router and end on a TDM DCS.

   a. True

   b. False

See Topic 3

8. What type of protection is supported in GMPLS?

   a. End-to-end

   b. Spam

   c. Both a and b

   d. Neither a nor b

See Topic 3

9. Which GMPLS concept helps with addressing the latency in the switch-fabric configuration of optical networks?

    a. Heirarchical LSPs

    b. Link bundling

    c. Suggested label

    d. All of the above

See Topic 3

10. Each LSP in a bidirectional LSP may have different bandwidth capacities.

    a. True

    b. False

See Topic 3

11. Which protocol is designed to localize faults in GMPLS networks?

    a. RSVP–TE

    b. OSPF–TE

    c. LMP

    d. Transmission control protocol (TCP)

See Topic 2

Glossary

ADM
Add/Drop Multiplexer

ATM
Asynchronous Transfer Mode

BLSR
Bidirectional Line-Switched Ring

CR–LDP
Contraint-Based Routing—Label Distribution Protocol

DCS
Digital Cross-Connect System

DWDM
Dense Wavelength Division Multiplexing

GMPLS
Generalized Multiprotocol Label Switching

IS–IS–TE
Intermediate System–to–Intermediate System—Traffic Engineering

LMP
Link-Management Protocol

LSP
Label-Switched Path

LSR
Label-Switched Router

OSPF–TE
Open Shortest Path First–Traffic Engineering

OXC
Optical Cross-Connect System

PXC
Photonic Cross-Connect System

QoS
Quality of Service

RSVP–TE
Resource Reservation Protocol–Traffic Engineering

SONET
Synchronous Optical Network

STS
Synchronous Transport Signal

TDM
Time Division Multiplexing

UPSR
Unidirectional Path-Switched Ring

VCC
Virtual Channel Connection

VT
Virtual Tributary