PERFORMANCE MEASURES OF INTEGRATED AUTOMATICALLY SWITCHING OPTICAL NETWORKS/GMPLS

,M.Deepika[1,] J.Gayathri[2],D.Ramyalakshmi[3],D.Uma[4]

[1] *Assistant professor,Electronics and Communication Department,Prince Shri Venkateshwara Padmavathy Engineering College,Tamilnadu,India*

[2] *Assistant professor,Electronics and Communication Department,Prince Shri Venkateshwara Padmavathy Engineering College,Tamilnadu,India.*

[3]*Assistant professor,Electronics and Communication Department,Prince Shri Venkateshwara Padmavathy Engineering College,Tamilnadu,India.*

[4]*Assistant professor,Electronics and Communication Department,Prince Shri Venkateshwara Padmavathy Engineering College,Tamilnadu,India.*

ABSTRACT

With the ever increasing growth of services and the corresponding demand for Quality of Service requirements that are placed on IP-based networks, the essential aspects of network planning will be critical in the coming years. A wide number of problems must be faced in order for the next generation of IP networks to meet their expected performance. With Performance Evaluation and Planning Methods for the Next Generation Internet for these developing trends, several new models are introduced that will lead to better Internet performance. One of the best solutions for meeting the Next –Generation Internet applications like Video-On-Demand, e-Science, RIA's Video conferencing and High Definition Television (HDTV) is the Optical Networks (ONS) which has a greater potential transmission, capacity than networking in the electrical domain. The core technology in ONS is Automatically Switching Optical Networks (ASON), which plays an important role in the dynamic routing on network connection. ASON routing protocol based on GMPLS includes the topology of optical network based on transmission of reach ability information. The Generalized Multiprotocol Label Switching is a protocol extending MPLS to manage further classes of interfaces and switching technologies. GMPLS comprises of three main protocols namely, 1.Signaling Protocol, 2.Routing Protocol and 3.Link Management Protocol (LMP). The signaling protocol in GMPLS process the exchanging of messages within the control plane to set up, maintain and modify the data paths. The protocol used for signaling is the Rsvp-TE that is sent between signaling controllers.The Routing protocol in GMPLS distributes the information that will be used as the basis of the path computation . The chief protocols used for routing are the OSPF-TE and IS-IS protocols. The link management protocol (LMP) overcomes problem of reducing the overhead errors and complexity in the network. The protocols used in LMP are the LDP and CRLD-TE. In this paper, we study and analyze the performance of various GMPLS sub protocols and their corresponding performance measures for future betterment.

Keywords: *Synchronous optical network, Multi-Protocol Label Switching, Automatically Switched Optical Network, Open Shortest Path First.*

1. INTRODUCTION-1:

As networks face increasing bandwidth demand and diminishing fiber availability, network providers are moving towards a crucial milestone in network evolution is the Optical Network. Optical networks are high capacity telecommunication networks based on optical technologies and components that provide routing, grooming and restoration at the wavelength level as well as wavelength-based services. Optical networks, based on the emergence of the optical layer in transport networks, provide higher capacity and reduced costs for new applications such as the Internet, video and multimedia interaction, and advanced digital services. The need for optical standards led to the creation of the synchronous optical network (SONET). It defines the types of network elements required, network architectures that vendors could implement, and the functionality that each node must perform. The one aspect of SONET that has allowed it to survive during a time of tremendous changes in network capacity needs is its

scalability. Based on its open-ended growth plan for higher bit rates, theoretically no upper limit exists for SONET bit rates. However, as higher bit rates are used, physical limitations in the laser sources and optical fiber begin to make the practice of endlessly increasing the bit rate on each signal an impractical solution. Additionally, connection to the networks through access rings has also had increased requirements. Customers are demanding more services and options, and are carrying more and different types of data traffic. To provide full end-to-end connectivity, a new paradigm was needed to meet all the high capacity and varied needs. Optical networks provide the required bandwidth and flexibility to enable end-to-end wavelength services. There are multiple standards bodies involved in developing control plane specifications for SONET/SDH network architectures. The ITU-T has defined a requirement which can be used to overcome this is an Automatically Switched Optical Network (ASON). ASON's vision is for complete network architecture with automated resource and connection management within the network, driven by dynamic signaling between the user and ASON network components. Since its introduction in the late 1990s, Multi-Protocol Label Switching (MPLS) has evolved into a hugely successful and flexible networking technology. The fundamental MPLS concept was to switch packets based upon looking up a label in the packet header. This label is swapped with a different label suitable for the next hop towards the packet's destination and it has been widely deployed on routers and switches. Subsequently, Generalized MPLS (GMPLS) expanded the concept of a label to include implicit attributes of the flow, such as wavelength of timeslot. This led to the adoption of GMPLS for circuit as well as packet switching, and it is widely deployed in such roles today. This paper mainly discusses about the working of GMPLS and the performance measures of its protocols.

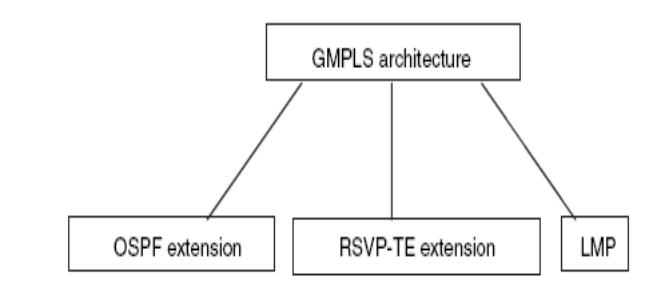


Fig -1 Major protocols used in GMPLS

2. GMPLS ROUTING PROTOCOL-2:

I.

GMPLS routing information distribution is based on extensions to IP routing protocols. Note that traffic engineering information distribution is currently limited to within an IP routing area — because there are two IP routing protocols that interoperate in a scalable way within an area (OSPF and IS-IS), both of these protocols were extended by the IETF. This paper introduces the extensions to the protocols in an abstract way before describing how the individual protocols were extended. In an IP network, routing is the process of determining the next hop for an IP packet on the shortest path toward its destination.

The chief routing protocols used within an area (OSPF and IS-IS) are link state protocols. Each router is responsible for distributing information about itself and its interfaces (that is, the local ends of its links). This information principally consists of the state of the link (active) and the cost of forwarding data through the router's interface onto the link. The information is distributed by the routing protocol to all routers in the area and each uses an algorithm to determine the open shortest path toward a destination, where ''open'' means that the links (interfaces) used are active and able to carry traffic, and ''shortest'' means least cost — that is, the sum of the costs of all the links to the destination is minimized.

2.1Open Shortest Path First(OSPF):

OSPF is an interior gateway protocol used for routing between routers belonging to a single Autonomous System. OSPF uses link-state technology in which routers send each other information about the direct connections and links which they have to other routers. Each OSPF router maintains an identical database describing the Autonomous System's topology. From this database, a routing table is calculated by constructing a shortest- path tree. OSPF recalculates routes quickly in the face of topological changes, utilizing a minimum of routing protocol

traffic. OSPF provides support for equal-cost multi-path. An area routing capability is provided, enabling an additional level of routing protection and a reduction in routing protocol traffic. In addition, all OSPF routing protocol exchanges are authenticated. It has been designed expressly for the TCP/IP internet environment, including explicit support for CIDR and the tagging of externally-derived routing information. OSPF also provides for the authentication of routing updates, and utilizes IP multicast when sending/receiving the updates. OSPF routes IP packets based solely on the destination IP address found in the IP packet header. IP packets are routed "as is" - they are not encapsulated in any further protocol headers as they transit the Autonomous System.OSPF enables the flexible configuration of IP subnets. Each route distributed by OSPF has a destination and mask. Two different subnets of the same IP network number may have different sizes (i.e., different masks). This is commonly referred to as variable length sub netting. A packet is routed to the best (i.e., longest or most specific) match.

8	**16**	**32 bit**
Version No.	Packet Type	Packet length
Router ID		
Area ID		
Checksum	AuType	

Fig -2 Protocol Structure - OSPF (Open Shortest Path First

Authentication (64 bits)

- Version number - Protocol version number (currently 2).
- Packet type - Valid types are as follows:
  - 1 : Hello
  - 2 : Database Description
  - 3 : Link State Request
  - 4 : Link State Update
  - 5: Link State Acknowledgment.
- Packet length - The length of the protocol packet in bytes. This length includes the standard OSPF header.
- Router ID - The router ID of the packet's source. In OSPF, the source and destination of a routing protocol packet are the two ends of an (potential) adjacency.
- Area ID - identifying the area that this packet belongs to. All OSPF packets are associated with a single area. Most travel a single hop only.
- Checksum - The standard IP checksum of the entire contents of the packet, starting with the OSPF packet header but excluding the 64-bit authentication field.
- AuType - Identifies the authentication scheme to be used for the packet.
- Authentication - A 64-bit field for use by the authentication scheme.

The current routing protocols typically used in an IP/MPLS network are OSPF (Open Shortest Path First) or IS-IS (Intermediate System to Intermediate System). In a GMPLS network, the OSPF that has been utilized in IP network is extended. In the OSPF extension, such concepts as a traffic-engineering (TE) link, hierarchization of the LSP, unnumbered links, link bundling and LSA (link-state advertisement) were introduced. In a GMPLS network, as illustrated by the hierarchization in Figure 4, a lower-layer LSP can become a link of an upper-layer LSP. For example, when an LSP is set on a certain TDM path, the TDM path behaves like a fixed link that has been there permanently for a long time. When the lower-layer LSP is set, the originating node of the LSP, when viewed from the upper layer, is advertised within the network as an upper-layer link. This LSP is called a TE link.

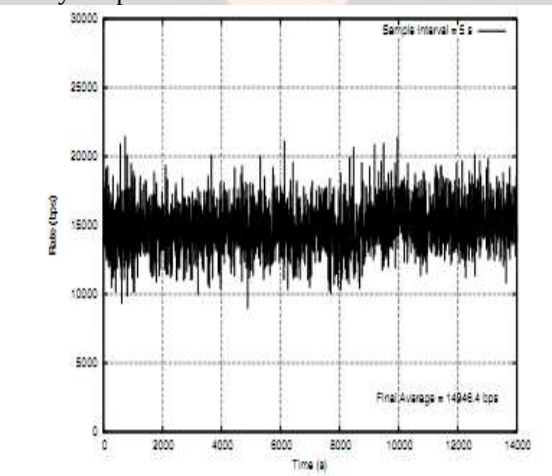
2.2 PERFORMANCE MEASURES OF ROUTING PROTOCOL:

The link state routing protocol function gives a routing controller the ability to introduce a new TE link, or to withdraw a TE link from service. It does the latter, for example, when it becomes aware that a fiber has failed or that an interface card has been pulled. This information is important to the signaling function because it means not only that no new LSP should be computed to use the failed TE link, but that all existing LSPs that use the link are broken. But it is also useful to define a half-way state between active and failed. In this state all existing LSPs can continue to function normally, but no new LSP should be attempted. This state can actually be achieved quite simply using the parameters. All that a routing controller needs to do to prevent new LSPs being signaled is to advertise that there is no more available bandwidth on the link (that is, that the maximum bandwidth that may be allocated to a new LSP is zero). There is concern that this process does not quite prevent all new LSPs. Suppose a ‘‘best effort’’ LSP was requested with zero reserved bandwidth: Wouldn’t it be possible to compute a path that used TE links for which all of the bandwidth had been withdrawn as described above? This is certainly the case, although it really only applies to packet switched links, because requesting a zero bandwidth timeslot or lambda is meaningless. One suggested option to handle this case is to use the GMPLS routing parameter that defines the minimum LSP bandwidth that may be allocated on the TE link — if this is set to some non-zero figure then a TE link with zero available bandwidth will not be available for any LSP. An alternative that is being discussed in the IETF’s CCAMP working group is to extend the GMPLS routing information by presenting a new flag that says ‘‘active, but no new LSPs allowed.’’

Obviously this process requires a small signaling extension to notify the services that the TE link is going out of service, but this is very easily achieved using new error codes for existing signaling messages.

Various suggestions have been made to summarize TE and GMPLS information so that it can be ‘‘leaked’’ from one domain to another. The idea is that this summarization would be a considerable reduction compared with the full TE information and would, therefore, perhaps be acceptable without compromising the function or the routing protocols. Two approaches have been suggested. One summarizes a domain as a virtual node presenting all of its external TE links and defining limited cross-connection abilities between these external TE links across the summarized domain. The other approach summarizes the domain as a set of edge-to-edge TE links.

Neither suggestion is, as yet, well developed, although some work has been suggested to add TE extensions to the inter-AS routing protocol, BGP. Instead, work is focusing on the Path Computation Element (PCE) that provides a proxy path computation server. To compute a path that leaves a domain, a request may be sent to the external PCE, and it may have wider visibility or may cooperate with PCEs from other domains in order to determine the best path.



Control Plane overhead related to OSPF-GMPLS traffic.

3.SIGNALLING PROTOCOL:

Signaling protocolsare responsible for provisioning, maintaining, and deleting connections. Optical networks are characterized by connection-oriented paradigms that require a resource reservation protocol. State-of-the-art control plane technologies operating on traditional IP-based networks focus on soft-state protocols that require periodic refresh throughout the participating nodes. In optical networks, where the data plane is separated from the control plane, a possible solution is also to adopt a hard state reservation protocol without periodic refresh to limit

the effect caused on the data plane by a failure in the control plane. Furthermore, redundant, generalized label binding is encouraged to reserve protection paths in the mesh network. Signaling messages are exchanged between software components called signaling controllers throughout the network. Each signaling controller is responsible for managing the data plane components of one or more data switches. In GMPLS the data switches are called Label Switching Routers (LSRs) and it is usual for the signaling controller to be present on the LSR so that the whole forms a single unit within the network. However, the GMPLS architecture supports two divergences from this collocation: First, the signaling controller may be physically diverse from the data switch, with a management or control protocol used to communicate between the two; secondly, a single signaling controller may manage more than one data switch.

Signaling controllers communicate with their neighboring signaling controllers through control channels in the control plane. A control channel is a link, which may be physical or logical, between signaling controllers responsible for data switches that are adjacent in the data plane. Signaling controllers that are linked by a control channel are described as adjacent (even though they might not be physically adjacent) and, once they are communicating with each other using the signaling protocol, they have established a signaling adjacency.

Control channels may utilize the data links between a pair of LSRs. In this case the signaling messages are mixed in with the data, and the control channel is described as in band. This is the case, for example, in mixed IP and MPLS networks.

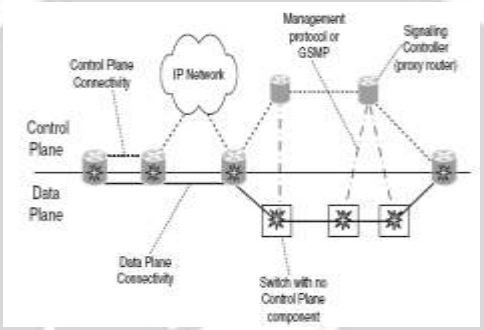


Fig-3 Possible configurations of signaling controllers and data switches

3.1RSVP-TE: Resource Reservation Protocol - Traffic Extension

The RSVP-TE protocol is an addition to the RSVP protocol for establishing label switched paths (LSPs) in MPLS networks. The extended RSVP protocol (RSVP-TE) supports the instantiation of explicitly routed LSPs, with or without reservations. RSVP-TE also supports smooth rerouting of LSPs, preemption, and loop detection. RSVP-TE defines a session as a data flow with a particular destination and transport-layer protocol. When RSVP and MPLS are combined, a flow or session can be defined with greater flexibility and generality. The ingress node of an LSP (Label Switched Path) uses a number of methods to determine which packets are assigned a particular label. Once a label is assigned to a set of packets, the label effectively defines the flow through the LSP. Such an LSP is an LSP tunnel because the traffic through it is opaque to intermediate nodes along the label switched path. New RSVP Session, Sender and Filter Spec objects, called LSP Tunnel IPv4 and LSP Tunnel IPv6 have been defined to support the LSP tunnel feature.

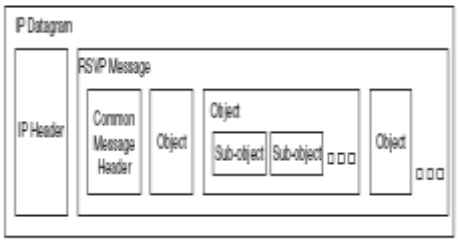


Fig-4 Block diagram of IP Datagram

A GMPLS RSVP-TE message is carried in an IP datagram and is constructed from a common header and a series of objects.In some applications it is useful to associate sets of LSP tunnels, such as during reroute operations or in spreading a traffic trunk over multiple paths, which sets are called traffic engineered tunnels (TE tunnels). To enable the identification and association of the LSP tunnels, two identifiers are carried. A tunnel ID is part of the Session object. The Session object uniquely defines a traffic engineered tunnel. The Sender and Filter Spec objects carry an LSP ID. The Sender (or Filter Spec) object, together with the Session object, uniquely identifies an LSP tunnel.

3.2 PERFORMANCE MEASURES OF SIGNALLING PROTOCOL:

Three additional tools enhance the ability to signal across multiple domains in GMPLS. The first allows ingress to specify exclusions from a path. This is useful because, when only a loose hop is used in the explicit path, the ingress has no other way to restrict which links and nodes are included within the path. If, for example, the ingress knows that a particular link is unreliable, or is aware of the path of another LSP that supports the same service, it may wish to inform the downstream LSRs that will expand the loose hop of the links and nodes to avoid. This is done by the inclusion of a new message object, the Exclude Route object, which provides GMPLS Signaling a global list of links and nodes to exclude; or by the inclusion of special exclusion sub-objects within the Explicit Route object.

The second utility adds support for crank back routing within GMPLS signaling. Crank back routing is not new, and has been used in PNNI and TDM networks. It facilitates ‘‘trial-and-error’’ progression of signaling messages across a multi domain network. When an LSP setup request is blocked because of the unavailability of suitable resources on a path toward the destination, an error report (LSP Upstream Error) is returned with a description of the problem. A new path computation may be attempted excluding the blocking links, nodes, or domains. Note that the use of crank back routing within a single domain approximates to random-walk routing and is not recommended, and the same can be said of a path that crosses many domains. Hierarchical (nested) and stitched LSPs provide the third building block for support of inter-domain LSPs.

Another solution to the computation of the path of an inter-domain LSP is provided by the Path Computation Element (PCE).

4 LINK MANAGEMENT PROTOCOL (LMP)

The Link Management Protocol (LMP) is a point-to-point application protocol that is run over UDP using port 701. This means that the LMP messages are scoped just to the single exchange between GMPLS devices that are adjacent in the data plane, and that the protocol must take responsibility for recovering from control plane errors because UDP is an unreliable transport protocol.LMP requires that the addresses of control channels are configured at each node. In order to maintain an LMP adjacency, it is necessary to have at least one active control channel between the two nodes. It is acceptable to have more than one control channel to provide a degree of robustness. In LMP the Node ID is usually taken from the IGP that is running in the network. In any case it should be globally unique, and must be sufficiently unambiguous to allow any one node to distinguish its peers.

4.1 LDP: Label Distribution Protocol Overview

In the MPLS networkLabel Distribution Protocol (LDP) is a key protocol, 2 label switching routers (LSR) must agree on the meaning of the labels used to forward traffic between and through them. LDP defines a set of procedures and messages by which one LSR (Label Switched Router) informs another of the label bindings it has made. The LSR uses this protocol to establish label switched paths through a network by mapping network layer routing information directly to data-link layer switched paths. Two LSRs (Label Switched Routers) which use LDP to exchange label mapping information are known as LDP peers and they have an LDP session between them. In a single session, each peer is able to learn about the others label mappings, in other words, the protocol is bi-directional.

4.2 CR-LDP: Constraint-based Label Distribution Protocol Overview

CR-LDP, constraint-based LDP, is one of the protocols in the MPLS architecture. CR-LDP contains extensions for LDP to extend its capabilities such as setup paths beyond what is available for the routing protocol. For instance, an LSP can be setup based on explicit route constraints, QoS constraints, and other constraints. Constraint-based routing (CR) is a mechanism used to meet Traffic Engineering requirements. These requirements are met by extending LDP for support of constraint-based routed label switched paths (CR-LSPs). Other uses for CR-LSPs include MPLS-based VPNs.

2 bytes	**2 bytes**
Version	PDU Length
LDP Identifier (6 bytes)	
LDP Messages	

Fig -5 Protocol Structure - LDP Label Distribution Protocol

Version -- LDP version number. The present number is 1.

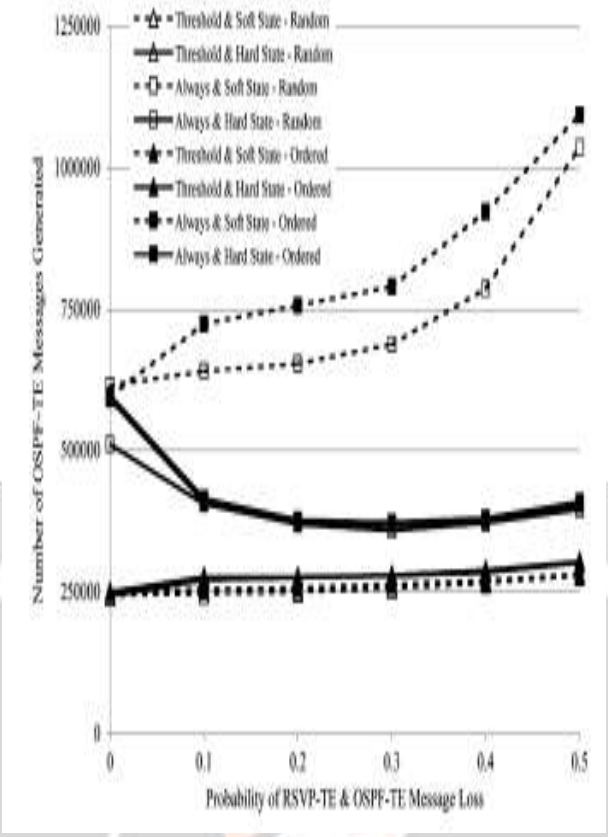
- PDU Length -- The total length of the PDU excluding the version and the PDU length field.
- LDP identifier -- This field uniquely identifies the label space of the sending LSR for which this PDU applies. The first 4 octets encode the IP address assigned to the LSR. The lst 2 indicate a label space within the LSR.

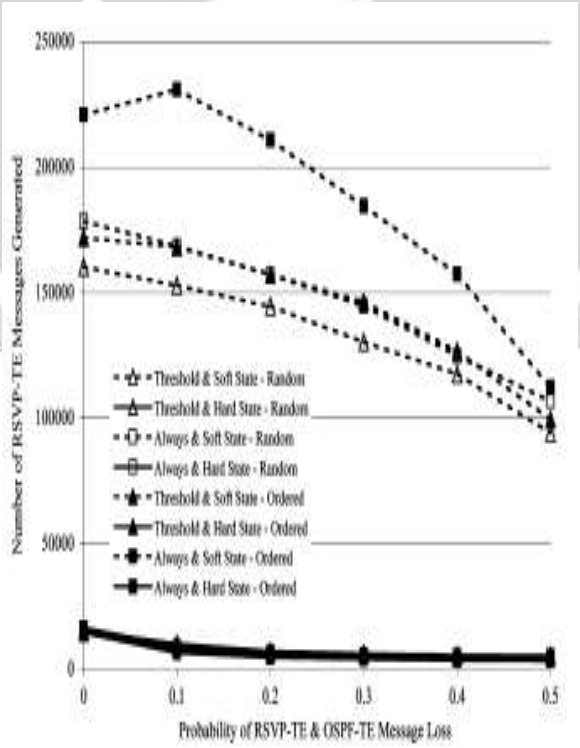
4.3 Performance measures of LMP:

Confidentiality is not considered a requirement of LMP, but it is necessary to authenticate message senders to protect against spoofing that might disrupt data services. This is especially important where the control channel passes through an arbitrary IP cloud on its way between two nodes that are adjacent in the data plane. The LMP specification suggests that LMP security is in the domain of the IP and UDP transport mechanisms and recommends the use of IPSec.

5. CONCLUSIONS AND FUTURE WORK

GMPLS is typically viewed an attractive, intelligent control plane for optical networks and this paper has studied the impact of faults in this control plane on the data plane by considering the impact of the loss of control messages from the two key GMPLS protocols, OSPF-TE and RSVP-TE. A number of configuration of these protocols were compared in a range of scenarios, with the impact of control message loss assessed through the evaluation of the efficacy of the control plane to establish and maintain data plane connections and the overhead incurred in doing so. In the scenarios considered, it was discovered that the loss of RSVP-TE messages is typically more consequential and is, in fact, often the determining factor in the overall performance. Soft-state RSVP-TE configuration tend to perform better than hard-state configuration, although the protocol overhead is larger. Furthermore, it was found that the hard state configuration often exhibit a rapid degradation in performance with rising message loss probability. Given the increasing tendency to use RSVP-TE as a hard-state protocol, these finding suggest that using the standardized optional retransmission algorithm is strongly recommended and, further, the algorithm's parameters should be conservatively set to ensure that all intended connections are established.It was discovered that the inherent reliability of OSPF-TE, due primarily to the flooding mechanism and the retransmission of unacknowledged messages, means the protocol is extremely resilient to control message loss, although the cost of this resilience is often significant protocol overhead for high message loss. It was found that the mechanism used to trigger the generation of OSPF-TE messages becomes increasingly important as the scarcity of the data plane resource being advertised increases. In fact, the best performance was observed by schemes that produce the greatest number of OSPF-TE messages suggesting that, in addition to resolving the usual performance/overhead tradeoff judiciously, there is a need to consider the scalability of OSPF-TE carefully, especially as the scarcity and volatility of data plane resource being advertised increases. There are many other interesting avenues for future work that emerge from the finding in this paper. Although the uniform randomly distributed loss of Studying the impact of control plane node failures directly is also attractive as it affords the opportunity to assess the recovery mechanisms that have been proposed and standardized and, importantly, to consider mechanisms to en- sure the presence of a faulty node does not degrade the overall


Threshold & Soft State - Random
Threshold & Hard State - Random
Always & Soft State - Random
Always & Hard State - Random
Threshold & Soft State - Ordered
Threshold & Hard State - Ordered
Always & Soft State - Ordered
Always & Hard State - Ordered
Number of OSPF-TE Messages Generated
1250000
1000000
750000
500000
250000
0
0
0.1
0.2
0.3
0.4
0.5
Probability of RSVP-TE & OSPF-TE Message Loss


Number of RSVP-TE Messages Generated
250000
200000
150000
100000
50000
0
Threshold & Soft State - Random
Threshold & Hard State - Random
Always & Soft State - Random
Always & Hard State - Random
Threshold & Soft State - Ordered
Threshold & Hard State - Ordered
Always & Soft State - Ordered
Always & Hard State - Ordered
0
0.1
0.2
0.3
0.4
0.5
Probability of RSVP-TE & OSPF-TE Message Loss

6.REFERENCES:

[1] Naoaki Yamanaka, Kohei Shiomoto and Eiji Oki, "GMPLS Technologies," Broadband backbone networks and systems, NTT Tokyo, Japan ,2006.
[2] Adrian Farrel and Igor Bryskin,"GMPLS Architecture and Applications,", San Francisco,2006.
[3] A. Jajszczyk, "Automatically switched optical networks: Benefits and requirements," IEEE Commun. Mag., vol. 43, pp. S10–S15, Feb. 2005.

[4] L. Velasco et al., "GMPLS-based multidomain restoration: Analysis, strategies, policies and experimental assessment," IEEE/OSA J. Opt. Commun. Newt. vol. 2, no. 6, pp. 427–441, Jun. 2010.

[5] OIF2002.23.06.Domain to Domain Routing Using GMPLSOSPFExtensions Vl.l (Draft), 2002.

[6] K. Kompella and Y. Rekhter, "OSPF Extensions in Support of Generalized Multi-Protocol Label Switching (GMPLS)," RFC4203 (Proposed Standard), Oct. 2005. [Online]. Available: http://www.ietf.org/rfc/rfc4203.txt

[7] L. Berger, "Generalized Multi-Protocol Label Switching (GMPLS) Signaling Resource ReserVation Protocol-Traffic Engineering (RSVP-TE) Extensions," RFC 3473 (Proposed Standard), Jan. 2003, atualizadapelas RFCs 4003, 4201, 4420. [Online]. Available: http://www.ietf.org/rfc/rfc3473.txt

[8] J. Lang, "Link Management Protocol (LMP)," RFC 4204 (Proposed Standard), Oct. 2005. [Online].Available: http://www.ietf.org/rfc/rfc4204.txt

[9] Norashidah Md. Din. Fuzzy Logic Traffic ControlForDifferentiatedService-Aware Generalized Multiprotocol Label Switching Network. PhD Thesis. University Technology Malaysia; June 2007.

[10] Network Node Interface for the Synchronous Digital Hierarchy (SDITU. Rec. G.707/Y.1322, Aug. 2003.

[11] "ITU. Rec. G.8080/Y.1304: Architecture for the automatically switched optical network (ASON)," Nov. 2001.