Leveraging IP Signaling and Routing to Manage UPSR-based Transport Networks

Vishal Sharma, Metanoia, Inc.
Abhimanyu Das and Charles Chen, Mahi Networks, Inc.

***Abstract* - An important requirement in the IP-based control of TDM optical transport networks is to utilize the in-built protection capabilities of SONET Unidirectional Path Switched Rings (UPSRs) and automate UPSR protected path setup in mixed mesh-ring networks. This requires modifications to existing IP signaling and routing protocols and new processing rules at the network nodes. In this paper, we leverage IP routing and signaling techniques and MPLS fast-reroute to accurately advertise UPSR ring topologies to remote nodes and dynamically establish UPSR protected paths across a transport network. Our proposal also makes a NUT[1]-like feature possible in UPSRs, which allows for efficient utilization of UPSR protection bandwidth. We achieve this by encoding UPSR specific information in the Opens Shortest Path First (OSPF) link state advertisements and in Resource Reservation Protocol (RSVP) signaling messages. In addition, we modify the signaling and routing state machines at the nodes to interpret and process this information to perform UPSR topology discovery and path computation. The uniqueness of our proposals is that the algorithms and the rules specified in the paper allow for existing IP-based protocols (such as those within the GMPLS framework, which currently applies to mesh networks) to be efficiently adapted for this context, while still achieving our objective of exploiting UPSR protection capabilities.**

I. Introduction

As IP-based signaling and routing protocols are adopted for the dynamic control of optical TDM networks, it is imperative that they account for the large installed base of SONET UPSR (Unidirectional Path Switched Rings)[1] and BLSR (Bidirectional Line Switched Rings)[2] rings. Thus, in mixed mesh-ring networks, the IP-based control protocols must allow for the automatic establishment of SONET channels, while utilizing SONET ring protection capabilities. In this paper, we take a pragmatic approach and focus on SONET Unidirectional Path Switched rings. This is motivated by the interworking possibilities offered by UPSRs today (which is much more difficult, if not non-existent, in BLSRs). Thus, mixed mesh-ring networks with UPSRs are good initial candidates for the application of dynamic IP control to transport networks. As such, fully solving the topology distribution and path setup problem for UPSRs is an important first step.

There are two important issues to consider when using IP protocols to manage and control legacy SONET ring networks. The first is to advertise the transport ring topology using IP routing protocols in a way that allows for path computation at each network node. This involves advertising information about both the working and protect fibers of a ring and enabling a remote node to distinguish between working and protection bandwidth. The second issue is to dynamically establish the ring-protected paths using IP-based signaling protocols. This involves automating the establishment *simultaneously* of *both* the working and the protection path. We solve both these issues in this paper.

We begin with a brief background of UPSR protection and of the IP-based protocols being defined for the dynamic control of transport networks.

A. UPSR Architecture

Ring topologies are by far the most widely deployed SONET network topology, and a common ring protection/restoration scheme in use today is UPSR protection.

A UPSR is a survivable, closed-loop, transport architecture that protects against fiber cuts and node failures by providing duplicate, geographically diverse paths for each circuit [1]. Adjacent nodes on the ring are connected using a single pair of optical fibers, which form two counter rotating rings carrying traffic in opposite directions (see [1]). Thus, working traffic travels in one direction (say, clockwise) on one fiber, while a protection path is provided in the opposite direction over the other fiber. A source sends traffic in both directions around the ring, so a UPSR can be used to provide a fully protected end-to-end path on a ring. Protection paths are set up and reserved when the working path is set up. In UPSR networks, the destination node on the ring monitors transmission on both fibers and performs a protection switch to the alternate path if it detects degraded (or loss of) transmission. Thus, switching between fibers is immediate with no loss of data, and no communication is needed with the transmitter.

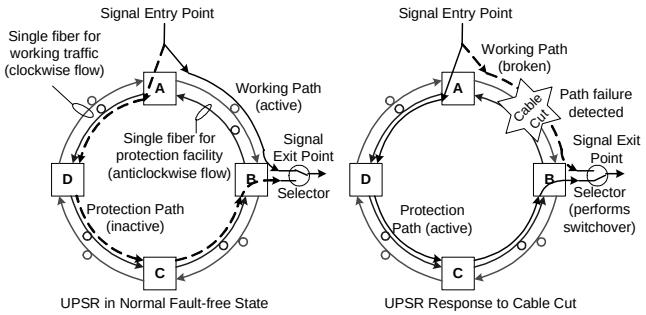

Figure 1. SONET UPSR protection switching architecture

The UPSR is an economical choice for most access and smaller metro applications, because its protection switching

[1] Non-preemptable Unprotected Traffic, a feature commonly offered in more expensive and more complex 2F and 4F BLSR systems.

mechanism is much simpler than that of 2-Fiber or 4-Fiber BLSRs and unlike the 4-Fiber BLSR it requires only two fibers to operate.

B. GMPLS Protocol Suite

Generalized Multi-Protocol Label Switching (GMPLS) extends the MPLS [5] concept of label switched paths and its traffic engineering capabilities to the control of TDM, lambda, and fiber switched networks [6]. GMPLS aims to provide a single, unified control plane architecture for multiple switching layers, by adapting existing MPLS signaling [3] and IP routing protocols [4] for non-IP transport networks [8]. This requires several modifications to the network elements and the IP protocols. First, it requires that the transport network elements have IP-based control channels for inter-element message transport. Second, to instantiate lambda/TDM circuits in addition to IP label switched paths (LSPs) the GMPLS protocol suite needs to extend IP signaling protocols. Similarly, to advertise link and node properties and other constraints (such as end-point switching and link protection capabilities) important in TDM transport networks, the suite needs to extend IP routing protocols. A reader interested in understanding these issues in the context of SDH/SONET networks is referred to [9]. Several of these extensions are being pursued in standards bodies, such as the IETF [10], [11].

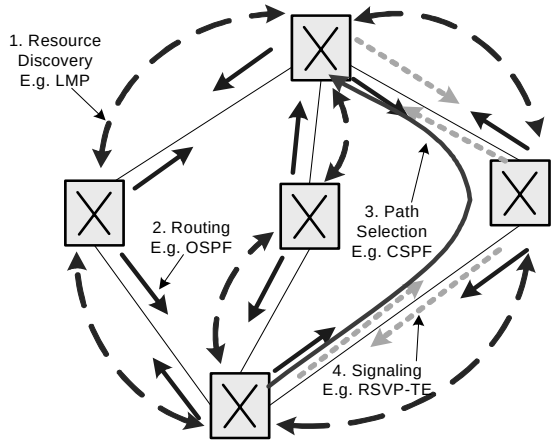

Figure 2. GMPLS: Basic architectural components

When applying IP-based protocols from data networks to IP-controlled transport networks, a key difference is the following. In the packet domain, the forwarding of data (IP data packets) and control information (IP signaling and routing protocol packets) is inherently on the *same* channel. In the transport domain, however, there is a natural separation of the control and forwarding planes. Further, the forwarding plane is circuit switched, while the control plane is packet switched. To allow for resilient IP-controlled transport networks, we therefore need to look at not only the data channels, but also the control channels. In this paper, we only address the protection of the data channels in the forwarding plane. The issues of control plane redundancy, while extremely important, are very different and are not dealt with here.

II. Motivation and Related Work

The current optical transport network in North America has a very large preponderance of SONET rings, over 100,000 [14] at last reckoning, amounting to billions of dollars in capital investment. There are also an equal number of SDH rings deployed across the world, representing a similar investment. A large fraction of these rings in the access and metro environments are UPSRs (or their SDH counterparts). Therefore, any attempt to automate the provisioning and control of optical transport networks must take this large installed base into account, and must be able to interwork seamlessly across the deployed UPSR infrastructure.

The GMPLS framework has been proposed within the IETF aims to automate the provisioning of paths in optical networks. While there has been significant work in this area, it has so far remained focused on mesh networks. Thus, even though the efforts under this framework extend the existing RSVP-TE [10]/CR-LDP signaling and OSPF-TE [11]/ISIS-TE routing protocols for dynamic path computation and path establishment in TDM and DWDM networks, they are geared at mesh topologies (perhaps because mesh topologies being conceptually similar to packet network topologies allow for a more natural application of IP protocols).

Clearly, it is not sufficient to automate merely the provisioning of paths over mesh topologies. In the absence of an integrated solution, path provisioning over rings continues to require the mostly manual TL1-based (Transaction Language 1; a language used to communicate with TDM switching equipment) configuration used today. The value of an automated control plane solution that can incorporate this existing equipment base, therefore, is tremendous.

Thus, the primary motivation behind our work is to develop a control plane solution that incoporates SONET UPSRs. By solving a very practical problem, our work makes it easier for service providers to move towards adopting an automated control plane for their transport networks. To the best of our knowledge we are not aware of any work that specifically addresses the issue of leveraging IP routing and signaling protocols to control *TDM ring networks*. As will be evident in the remainder of this paper, applying IP protocols to ring topologies requires a rethinking of the protocol extensions in the light of the properties of ring topologies.

For example, GMPLS signaling protocols [10] have defined the Protection Object/TLV to specify the type of protection (1+1, 1:1, unprotected, or enhanced, for example) desired by a LSP at *each hop* along its path. The protocol allows for a source to set multiple Link Flag bits in the Protection object to indicate which type of protection is acceptable for the LSP. This allows for LSP setup in networks where links may offer different levels of protection. However, the Protection object by itself is not sufficient to signal and establish an LSP with UPSR protection. For that it is also necessary to extend the signaling protocol to establish the protection segment of an

LSP on a UPSR in conjunction with its working segment, and to correlate the two segments.

One way to achieve this is to allow the *hub nodes*[2] of UPSR rings (for example, nodes 3 in Figure 3) to split a single connection request into *two* LSP establishment requests *within* a given UPSR ring, one to establish the working segment of the LSP and the other to establish the protect segment. Thus in Figure 3, Node 3 would be responsible for splitting the original request coming from Node 5 into two requests. The first would establish the working segment through nodes 4, 1, and 2, while the second would establish the protect segment through nodes 3 and 2. This suggests an adaptation of the RSVP-TE fast reroute techniques available for LSP setup in the IP domain [13], and is indeed an approach we discuss further in Section IV

Similarly, even though the current GMPLS routing enhancements to OSPF-TE have defined a Link Protection Type sub-TLV, it is not adequate to convey information about UPSR links such as whether they correspond to working or protect fibers, and which specific UPSR they belong to. So we need to specify additional enhancements to advertise and process UPSR link LSAs (Link State Advertisements) using OSPF-TE.

In the following sections, we will focus on how GMPLS RSVP-TE signaling and the corresponding processing rules may be extended to signal UPSR protected LSPs (Label Switched Paths), and on how GMPLS OSPF-TE processing may be extended to advertise links belonging to UPSRs, so that remote network nodes may build the topology of UPSRs in the network. Note that while we use OSPF and RSVP-TE as examples, our proposals are generic and can be applied to other routing and signaling protocols as well, such as IS-IS and CR-LDP.

The management and operation of UPSR-based transport networks is greatly enhanced using our proposals for dynamic IP-based configuration of UPSRs This is especially important considering the time-consuming, static per-node configuration using management systems that is largely prevalent today. Another important advantage of our proposal is that it allows for the provision of Non-preemptable Unprotected Traffic (NUT) on UPSR rings, which is not possible with traditional UPSR configuration. This is an important feature, usually associated with the more complex 2F-BLSR and 4F-BLSR networks. By advertising the SONET ring topology using our extensions to OSPF, this feature can also be made available on IP-controlled UPSR networks.

As we will see later, by suitably enhancing the GMPLS signaling and routing protocols, and by following a set of rules when distributing and interpreting link state advertisements, it is possible to enable UPSR-protected LSP setup within the current GMPLS framework. The remainder of this paper outlines our proposed enhancements, which enable the integration of UPSR ring protection without altering the base GMPLS protocols.

[2] We define a *hub node* on a UPSR ring to be a node that either originates or terminates a TDM LSP (or TDM channel/circuit) or one that sits at the intersection of two or more UPSR rings.

III. Enhancements to Routing Protocols and Path Computation

The goal of the routing enhancements is for every node in a mixed mesh-ring network to discover the *complete topology* of the network's UPSR rings. This means that, for each link, every node must be able to ascertain:

-Whether the link belongs to a UPSR, and if so

-The particular UPSR to which the link belongs, and

-Whether the advertised link corresponds to the working or the protect components of the UPSR.

To enable this, we propose enhancements to the sub-objects in GMPLS OSPF-TE, and a set of rules that every network node must follow to derive a consistent network topology from the LSAs (Link State Advertisements). The enhancements to OSPF-TE are as follows:

-- The OSPF-TE LSA must have a field to indicate the underlying *protection technology* to which a link belongs. Currently, this could be linear, UPSR, 2F-BLSR, 4F-BLSR, SNCP, or MS-SPRING. This ensures that a receiving node always knows the type of ring to which a link described by the LSA belongs. It also provides future extensibility, since new types of rings (such as optical rings) can also be incorporated easily by defining new code points for this field.

-- An optional "Ring ID" field must be added to the Protection sub-object and used in OSPF-TE LSAs describing *UPSR links* (shorthand for "links on UPSR rings"), so that links belonging to a given UPSR ring may be readily identified. This ensures that when multiple UPSRs are superimposed over the same set of physical nodes, this attribute will help remote nodes to easily distinguish between the links of different UPSRs.

-- UPSR link components that lie on the working and protect fiber respectively are distinguished by the link protection type sub-TLV. Link components on the working fiber are advertised using the "enhanced" link protection type, and those on the protect fiber using the "unprotected" link protection type.

Observe that advertising working and protect links in the manner described above differs semantically from the way in which links are treated in packet IP networks. IP assumes that each link is *physically and logically bi-directional* and *is advertised by LSAs in both directions*. In the UPSR case, a link between two nodes, while being physically bidirectional is inherently asymmetrical, since one direction of the link lies on the working fiber while the other lies on the protect fiber. Since IP-based protocols are used in the GMPLS framework, both the working and protect components of the link have the same end point identifier (IP address or unnumbered identifiers)[3], so they can only be distinguished by their direction. Yet they can have completely different TE metrics

[3] Note that when advertising a *physical* UPSR link, the working fiber and the protect fiber actually connect to the transmitter (Tx) and receiver (Rx) of a single physical transceiver at a node, and so have the same interface identifier (which could be an unnumbered interface identifier or an IP address, depending on how links in the network are numbered). Thus, in Figure 3 the link between node 1 and node 2 has only one identifier for each of the two components of the link: the outgoing working fiber and the incoming protect fiber.

(such as available bandwidth). Thus, the two LSAs generated by the opposite ends of this "link" actually describe individually the working and protect components of the link. The working and protect components of every UPSR "link" are not symmetrical and must therefore be advertised separately.

Yet another difference from normal IP networks is that IP assumes that reverse traffic between the end points of a link can be sent back over the *same* link. In the UPSR case, however, the reverse direction of a UPSR "link" lies on a protect fiber and *cannot* be used for sending working traffic in the reverse direction. Thus, even though each advertised UPSR "link" is physically bi-directional, the "reverse path" for sending traffic back to the source node is *not* over the same link, but rather over the remaining part of the ring. Thus, when creating the network topology form the OSPF-TE LSAs, a remote node must keep the logical unidirectional nature of working (and protect) components of a link in mind.

For example in Figure 3, node 3 will advertise router LSAs with three links, link(3,4), link(3,2) and link(3,5). Link(3,4) will describe the working segment of the UPSR link between nodes 3 and 4. Link(3,2) will describe the protect segment of the UPSR link between nodes 3 and 2, and Link(3,5) will describe a normal, linear, unprotected link between nodes 3 and 5. The protection technology sub-object and link protection type sub-object for link(3,4) will be *UPSR* and *enhanced* respectively, while for link(3,2) they will be *UPSR* and *unprotected*. For link(3,5), the sub-objects will be *Linear* and *Unprotected*, respectively. Note that the working segment of every UPSR link is advertised by the node at one end of the link, while the protect segment is advertised by the node at the other end.

To send traffic over the working path from Node 2 to Node 3, one will use the working component 2→3 of the UPSR link between nodes 2 and 3. To send working traffic back from Node 3 to Node 2, however, one must again use the same clockwise working fiber, and go via the working components of the links between nodes 3, 4, 2, and 1, in the order 3->4->1->2. The protect component 3→2 of the link between nodes 2 and 3 cannot be used. Therefore, a bi-directional "working traffic" link between nodes 2 and 3 is comprised logically of the working component 2→3 of the link between nodes 2 and 3 and the working components 3→4, 4→1, and 1→2 of the links between nodes 3, 4, 2, and 1.

One way to be consistent with the normal IP notion of bi-directionality would be to let both nodes 2 and 3 advertise a "virtual" bi-directional link between themselves (comprising working component 2→3 of the link between nodes 2 and 3, and the working components 3→4, 4→1, and 1→2 of the links between nodes 3 and 4, 4 and 2, and 2 and 1 respectively). In that case, a remote node receiving an LSA describing this "virtual" link from both the nodes could process the link just like a normal bi-directional link in IP. This, however, would complicate the advertising of TE-properties (e.g., available timeslots) of such a "virtual" link.

Finally, the changes to the rules for advertising and processing LSAs are as follows:

-- The working and protect components of a UPSR link must each be advertised in a separate LSA by the node from which the component emanates. Thus in Figure 3, for the UPSR link between nodes 2 and 3, the working component 2→3 will be advertised by node 2, while the protect component 3→2 will be advertised by node 3

-- All LSAs describing working or protect components of a UPSR link, must have the "UPSR" code point in the new OSPF protection technology sub-object.

-- The working component of a UPSR link must be advertised with the "enhanced" link protection type in the protection sub-object, while the protect component must be advertised with the "unprotected" link protection type.

-- The protection technology sub-object, the link protection type field, and the Ring ID together enable a remote node to completely identify the working and protect components of a UPSR's links. The topology that a remote node uses for calculating paths via SPF/CSPF for protected traffic (or traffic wishing to be routed over the protect fiber) must use only the LSAs corresponding to working components of UPSR links. However, when computing paths for LSPs willing to be routed over the protect components of UPSR links, a node may use LSAs that describe both the working and protect components of UPSR links.

Note that by advertising and processing the LSAs for the protect component of UPSR links separately, we enable a remote node to discover unused bandwidth on the protection channels, which can be used to route "extra" traffic.

The unused protect bandwidth may be either *preemptable* or *non-preemptable*. Preemptable bandwidth is bandwidth available on segments of the protect fiber for which there is corresponding unused bandwidth on appropriate segments of the working fiber. So, when a UPSR protected circuit that uses the corresponding timeslots is created on the working fiber, the extra traffic on the protect segment is preempted to create the UPSR protect circuit. Non-preemptable bandwidth is bandwidth on a segment of the protect fiber for which the corresponding bandwidth on an appropriate segment of the working fiber has been used to create an unprotected (non-UPSR) circuit, which will never make use of its corresponding timeslots on the protect segment. Thus, traffic using this bandwidth is unprotected, but non-preemptable, akin to NUT in 2Fand 4F BLSR.

Given these changes in LSA processing at the sending and receiving nodes (and some changes to signaling to be described in Section IV), a node can now treat the task of setting up a *UPSR protected TDM trail* as equivalent to setting up a *working LSP*, that is routed over the working fibers on the UPSRs in its path, and *detour LSPs* that are initiated by every ingress hub node and routed over the protect fibers on the UPSRs. The intermediate links taken by the working LSP can be explicitly specified at the source, by consulting its TE database. The path of the detour LSPs need not be specified and can be calculated by the respective hub nodes. Once the hub nodes on the path of the UPSR protected TDM trail can correlate the working and protect/detour LSPs, the end result is the same as if one had set up a single, manually provisioned, UPSR protected TDM circuit.

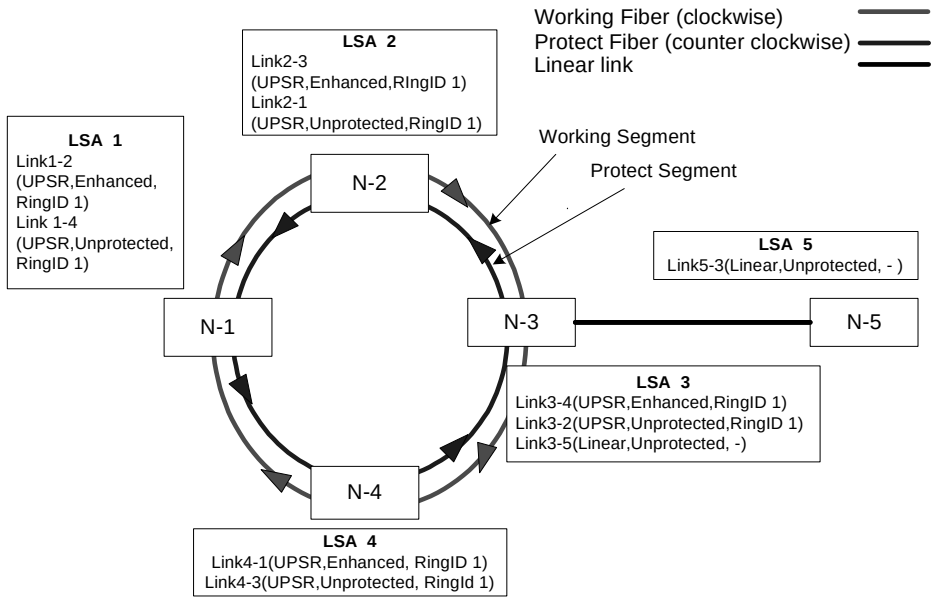

Figure 3. OSPF-TE LSA advertisements to enable correct UPSR topology inference at remote nodes.

Given these changes in LSA processing at the sending and receiving nodes (and some changes to signaling to be described in Section IV), a node can now treat the task of setting up a *UPSR protected TDM trail* as equivalent to setting up a *working LSP*, that is routed over the working fibers on the UPSRs in its path, and *detour LSPs* that are initiated by every ingress hub node and routed over the protect fibers on the UPSRs. The intermediate links taken by the working LSP can be explicitly specified at the source, by consulting its TE database. The path of the detour LSPs need not be specified and can be calculated by the respective hub nodes. Once the hub nodes on the path of the UPSR protected TDM trail can correlate the working and protect/detour LSPs, the end result is the same as if one had set up a single, manually provisioned, UPSR protected TDM circuit.

IV. Enhancements to Signaling Mechanisms and Protocols

The fundamental goal of the signaling enhancements is to setup a TDM trail using a single LSP setup from the source. In other words, the signaling should to be able to establish both the working and protect segments of the LSP over each UPSR that the trail crosses. This is accomplished by allowing the hub nodes on each intermediate UPSR to spawn a detour LSP [13] over the protect fiber, which sets up the protect segment corresponding to the working segment of the LSP. In essence, this helps localize the effect of failures, just as is the case for SONET channels established by configuration, since failures on intermediate UPSRs can now be handled locally.

Since the objective is to enable RSVP-TE to configure the cross connects at every node that a TDM trail passes through, an alternative would be to initiate two explicitly routed LSPs from the source itself, one of which takes the working segments while the other takes the protect segments. Even though this option requires fewer changes to the GMPLS signaling protocols, it is not a very robust solution. For one, the failure of *any* node along the working path would cause a switchover to the protection segments in all UPSRs that the trail was routed over. This is clearly unacceptable, and goes against the very essence of UPSRs, which is to localize the effect of failures. Secondly, for a TDM trail passing through two UPSRs, if the working segment on the first ring failed, and the protect segment on the second ring failed, both the working and protect LSPs would be torn down, thus bringing down the TDM trail, *even though* a path using the working segment in the first ring and the protect segment in the second ring would still be available to service the LSP.

Our signaling proposals work within the framework of the GMPLS protocols while using some RSVP-TE fast-reroute enhancements from the packet domain, but they still integrate SONET UPSR rings (and their protection capabilities) into the network.

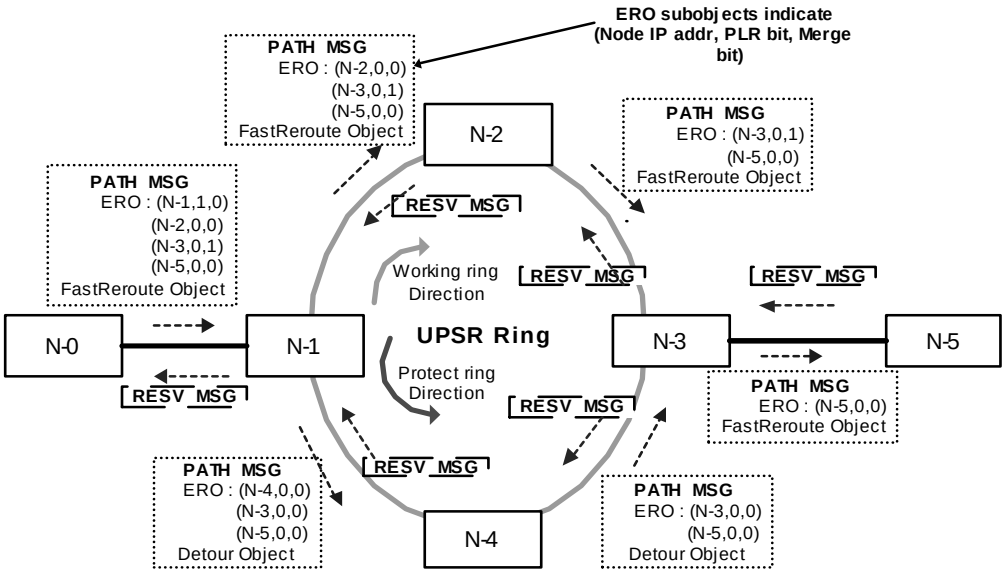

Figure 4. Setup of Working and Detour LSPs over UPSR ring topology, from Node 0 to Node 5 (PATH and RESV message flow).

A. Detour LSP Enhancements

We follow the same basic strategy as outlined in [13], where there is a Fast Reroute object in the primary LSP and a Detour object in the detour LSP. As in [13], the detour LSP is initiated at the points of local repair (PLRs), which are the ingress hub nodes in UPSRs, and is merged back at the Merge points, which are the egress hub nodes in UPSRs. The fast reroute proposal, however, has no provision for a source to specify the PLR and the Merge points, a functionality that is needed in the UPSR case to allow UPSR hub nodes to correctly setup working and protect paths. (Recall that the fast reroute proposal is designed for packet LSPs, where the objective is to protect as many nodes/links by local repair as possible. To enable this, we propose to use two bits (the "PLR" bit and the "MERGE" bit) in the ERO sub-object of the RSVP path message, which allows every node specified in the ERO at the source, to be marked as a MERGE or PLR node, if needed.

B. RSVP State Machine Enhancements at Hub Nodes

Our signaling enhancements are designed to minimize any change in normal processing of GMPLS RSVP-TE messages. The only changes necessary in RSVP-TE processing are at the UPSR hub nodes.

The ingress hub node on receiving a TDM trail setup request, checks for the presence of the Fast Reroute object to determine whether the TDM circuit is to be UPSR protected. If this object is present, the node further checks the ERO object to see if it is a designated PLR, and, if so, locates the very next merge point, which is the egress hub node on the current ring. Having done so, the node consults its TE database and constructs an ERO for the detour LSP that it uses to establish the protect path over the UPSR. The original LSP Path request continues over the working path specified in its ERO to set up the working UPSR circuit. Upon receiving labels from both the working and detour LSPs, the ingress hub node configures its UPSR hardware to enable swap-over for UPSR protection.

The egress hub node on receiving Path messages from both the working and detour LSPs, merges them and forwards only one LSP request downstream of itself, as specified in [13]. Upon receiving a Resv message from its downstream neighbor, the node sends Resv messages back individually for the working and detour LSP setup requests over the working and protect links, respectively. It also configures its UPSR cross-connects to enable UPSR protection on the two incoming links specified by the two LSP requests. Figure 4 shows an example of UPSR protected LSP setup in our example topology.

An important change that we make in the RSVP processing rules relative to [13] is that, every ingress hub node, when receiving an LSP Path message with the FastReroute object set (which indicates to the node to spawn off a detour LSP) for the first time, does not forward a Resv message upstream (towards the source), until it gets Resv messages from both the working and detour LSPs. Alternately, until it receives the first

Resv message from both working and detour LSPs, any Path-Error message it receives for either LSP is forwarded upstream. This is necessary so that if the detour LSP is unable to setup the protect path over a UPSR ring, the end-to-end LSP setup fails as well. Stated more formally, if a node detects that it is an ingress hub node/PLR and spawns a Detour LSP request, then it should send the *first* Resv message back upstream *only* when it receives a Resv message back from *both* the working and detour LSPs. This check is applied *only* for the first Resv message that the ingress hub node has to send back. Once the LSP is set up (that is, both the working and protect paths have been successfully created) any node failure on either the working or the protect LSP segment on the ring, but not both, should not tear down the overall LSP. So, after the LSP is up, a Path Error message at the ingress hub node received over either the working or the protect segment alone *should not* be forwarded upstream, *unless* a Path Error has been received from both segments of the LSP.

C. *Bi-directional Protected LSP Setup using Upstream Label Objects*

A bi-directional UPSR-protected LSP can be setup by including an UPSTREAM label in the detour LSP setup. Note that the usual paradigm for the UPSTREAM label does not apply here. The UPSTREAM label in the usual PATH message in GMPLS [11] is used to set up the reverse *working* path for a bi-directional LSP. In other words, the UPSTREAM label establishes a working path in the reverse direction to that corresponding to the direction of the PATH message (which is the direction of the forward working path).

However, in the UPSR case (see Figure 5), the UPSTREAM label in the RSVP Path message traveling on the working fiber (for setting up the *working* TDM LSP) will setup the *protect* LSP corresponding to the working path in the reverse direction. Similarly, the UPSTREAM label included in the detour object (for setting up the *protection* LSP for the forward working path) will setup the *working* LSP for the reverse working path.

V. Conclusion

In this paper, we have presented a comprehensive proposal to enable IP-based automated topology and resource discovery and path computation, and automated path establishment for UPSR transport networks. By suitably modifying the existing GMPLS signaling and routing protocols for mesh networks, and adapting the concepts of RSVP-TE fast reroute, we allow for the setting up of UPSR protected LSPs in mixed mesh-ring networks. In addition, by enabling a NUT-like feature for UPSRs, we have also provided a mechanism to use the protection bandwidth of the UPSR more efficiently. This is made possible by the novel bandwidth advertisement schemes we proposed and the signaling enhancements we developed.

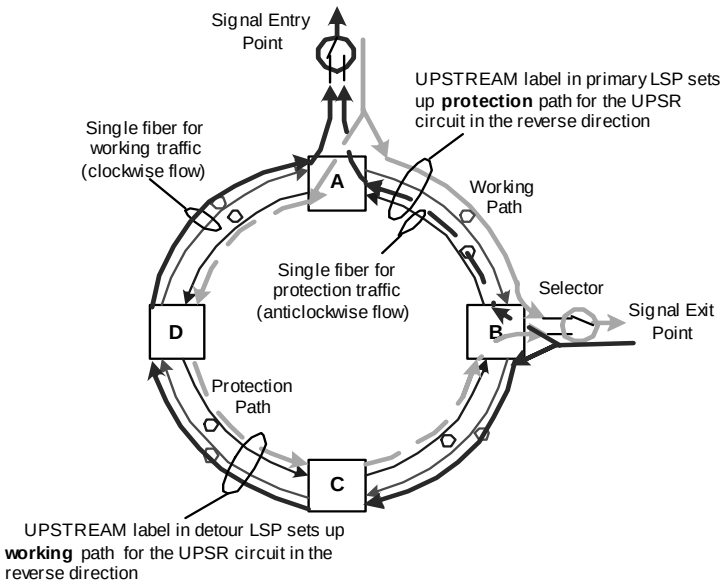

Figure 5. Illustration of bi-directional TDM LSP setup on a UPSR. Note the differences with the usual paradigm for the UPSTREAM label for bi-directional LSPs.

Several directions of future work are possible from here. One is to look at the issue of end-to-end protection of TDM trails. That is, protection and traffic engineering across areas and domains. The other is to consider how protection is handled in the case of multicast. With applications such as video conferencing and web casts, this will become increasingly important. Yet another would be to look at control plane redundancy, which is an important topic in its own right, and which we did not cover in the current paper. Finally, it would be useful to see how these notions can be generalized to apply to BLSRs.

References

[1] GR-1400-CORE, "SONET Dual-fed Unidirectional Path Switched Ring (UPSR) Equipment Generic Criteria, Issue 2, Bellcore, January 1999.

[2] GR-1230-CORE, "SONET Bi-directional Line Switched Ring (BLSR) Equipment Generic Criteria," Issue 4, Bellcore, December 1998.

[3] A. Bannerjee, J. Drake, J.P. Lang, B. Turner, K. Kompella, Y. Rekhter "Generalized Multi Protocol Label Switching: An overview of routing and management enhancements", *IEEE Commun. Mag.*, Vol. 39, Issue 1, January 2001, pp. 144-150.

[4] A Bannerjee, J. Drake, J.P. Lang, B. Turner, D. Awduche, L. Berger, K. Kompella, Y. Rekhter "Generalized Multi Protocol Label Switching: An overview of signaling enhancements and recovery techniques", *IEEE Commun. Mag.*, Vol. 39, Issue 7, July 2001, pp. 144-151.

[5] G. Swallow, "MPLS advantages for traffic engineering," *IEEE Commun. Mag*, Vol. 37, Issue 12, December 1999, pp. 54-57.

[6] D. Awduche, Y. Rekhter, “Multiprotocol Lambda Switching: combining MPLS traffic engineering control with optical crossconnects,” *IEEE Commun. Mag*, Vol. 39, Issue 3, March 2001, pp. 111-116.
[7] G.Bernstein, J. Yates, D Saha “IP-Centric Control and Management of Optical Transport Networks”, *IEEE Commun. Mag.*, Vol. 38, Issue 10, October 2000, pp. 161-167.
[8] Y. Xu, P.N. Lamy, E.L. Varma, R. Nagarajan “Generalized MPLS-Based Distribution Control Architecture for Automatically Switched Transport Networks”, *Bell-Labs Technical Journal*, Jan-June 2001.
[9] G. Bernstein, E. Mannie, V. Sharma, “Framework for MPLS-based Control of Optical SDH/SONET Networks,” *IEEE Network*, July/August 2001.
[10] L. Berger, et al, “Generalized MPLS – Signaling Functional Description,” Work in progress, draft-ietf-mpls-generalized-signaling-08.txt, April 2002.
[11] L. Berger, et al, “Generalized MPLS Signaling – RSVP-TE Extensions,” Work in progress, draft-ietf-mpls-generalized-rsvp-te-07.txt, April 2002.
[12] K. Kompella, et. al. "OSPF Extensions in Support of Generalized MPLS", Work in Progress, draft-ietf-ospf-gmpls-extensions-07.txt, May 2002.
[13] P. Pan, et. al. " Fast Reroute Extensions to RSVP-TE for LSP Tunnels”, Work in Progress, draft-ietf-mpls-rsvp-lsp-fastreroute-00.txt , January 2002.
[14] J. Duffy, “Intelligent services make MANs hot,” Network World, 8 May, 2000. http://www.nwfusion.com/news/2000/0508infra1.html