Traffic Engineering Working Group
Internet Draft
Expiration Date: January 2002

Ken Owens
Erlang Technology, Inc.
Vishal Sharma
Metanoia, Inc.

Mathew Oommen
Williams Communications

July 2001

Network Survivability Considerations for Traffic Engineered IP Networks

draft-owens-te-network-survivability-01.txt

Status of this Memo

Abstract

Network survivability refers to the capability of the network to maintain service continuity in the presence of faults within the network [1]. Recovering from network failures quickly and maintaining the required QoS for existing services can accomplish this1. With the increasing sophistication of network technologies, survivability capabilities are becoming available at multiple layers, allowing for protection and restoration to occur at any layer of the network. This makes it important to: scrutinize the recovery features of different

network layers, understand the pros and cons of performing recovery at each layer, and assess how the interactions between layers impact network survivability. With these objectives in mind, this draft examines the considerations for network survivability at different layers of the network.

Table of Contents Page

Abstract
1. Introduction Background
2. Overview of Survivability in Traffic Engineered Networks Background
3. Purpose of This Document Background
4. Motivation Background
5. Network Survivability Objectives Mostly design issues
6. Network Survivability Parameter Considerations OK - summarize
   6.1 Time-scale of Operations
   6.2 Resource Efficiency
   6.3 Signaling
   6.4 Recovery Granularity
   6.5 QoS Granularity
   6.6 Coverage
   6.7 Fault Monitoring and Reporting
   6.8 Interactions with Other Layers
7. Network Survivability Layer Considerations May be as appendix
   7.1 Optical Layer
   7.2 SONET/SDH Layer
   7.3 ATM and/or MPLS Layer
   7.4 IP Layer
   7.5 Transport Layers
   7.6 Coordination between Layers
8. Service Provider Considerations May be as appendix
9. Security Considerations
10. Acknowledgements
11. References
12. AuthorsÆ Addresses

1. Introduction

With the increasing demand to carry mission critical traffic, real-time traffic, and other high priority traffic over the public Internet [1], network survivability has become an issue of great concern for the Internet community. As network technologies continue to improve and converge, protection and restoration schemes are being developed at multiple layers.

At the lowest layer of the stack, optical networks are now becoming capable of providing dynamic ring and mesh restoration functionality as well as traditional 1+1 or 1:1 protection functionality. A considerable body of work in the research community has dealt with the capacity and efficiency considerations inherent in the layout of optical lightpaths for traffic protection, and work is ongoing [2],[3],[4],[5], [6] to develop a signaling framework to support even more sophisticated restoration features at the optical layer for future IP-over-WDM networks. Moving up the layered stack, the SONET/SDH layer provides

survivability capability with automatic protection switching (APS), as well as self-healing ring and mesh architectures. A similar functionality is provided by the ATM Layer, with work ongoing to also provide such functionality using technologies such as MPLS [7]. At the IP layer, rerouting is used to restore service continuity following link and node outages. Rerouting at the IP layer, however, occurs after a period of routing convergence, which may require from a few seconds to several minutes to complete.

Another important aspect of multi-layer survivability is that the various technologies operating at different layers provide protection and restoration capabilities at different temporal granularities (i.e., time scales), ranging from a few tens of milliseconds to minutes, at different bandwidth granularities (i.e., from packet-level to wavelength level), ranging from a few kilobits per second to hundreds of gigabits per second, and at different QoS granularities, ranging from aggregated traffic classes (e.g., diffserv classes) to individual traffic streams/flows (e.g., per VC or per-IP flow). It is, therefore, a challenging task to combine in a coordinated manner the different restoration capabilities available across the layers to ensure that certain network survivability goals are met for the different services supported by the network.

2. Overview of Survivability in Traffic Engineered Networks

Traditional IP networks supported only one class of service, the best-effort class, and focused primarily on connectivity. Network survivability in such an environment merely involved the restoration of network connectivity, which was provided by layer 3 re-routing alone and was acceptable, since this was all that was needed. -A concern with relying on the routing algorithms alone was the time that the routing algorithms took to converge and restore service could be significant, on the order of several seconds to minutes, causing a disruption of service in the interim. Even though this was not a concern with best-effort traffic, it does become a significant concern when the aim is to provide applications requiring highly reliable service, where the recovery times must be in the order of tens of milliseconds.

With the increasing need for explicit engineering of network traffic loads, however, it has become imperative for traffic engineering mechanisms to take network survivability considerations into account. An important objective of contemporary and future Internet traffic engineering, in fact, is to facilitate reliable network operations by providing mechanisms that enhance network integrity and by adopting policies that accommodate network survivability [1]. This is important for two reasons. First, to minimize the vulnerability of the network to service outages arising from errors, faults, and failures that occur within the infrastructure. Second, to optimize the performance of operational IP networks by rapidly converging to a stable state while not even letting TCP stacks know about the failure.

Network faults, be they link outages (fiber cuts, transmitter failures, etc.) or node outages (mis-configuration, processor or line card failures, power glitches, power supply failures, etc.), will continue to be a fact of life that network engineering will have to accommodate. Whereas in the past this only meant ensuring that network connectivity

was restored following an outage, in current networks it means ensuring that network connectivity is restored within certain constraints and performance levels so as not to affect the services transported. Thus, any traffic-engineered network that carries critical, high-priority traffic needs to be resilient to faults. Indeed, an engineered network that is not survivable cannot be said to be truly traffic engineered, since faults in the network elements could create traffic imbalances that the network is not geared to handle, thereby severely compromising the performance of the network.

A major objective of Internet traffic engineering is to enhance the performance of an operational network at both the traffic and resource levels. This is accomplished by addressing traffic-oriented performance requirements, while utilizing network resources efficiently, reliably, and economically. Traffic oriented performance measures include delay, delay variation, packet loss, and goodput [1]. The scope and nature of survivability required in different parts of the network should form an integral part of the traffic engineering process model. In fact, survivability requirements would influence the first (definition of relevant control policies), third (analysis of network state to characterize traffic workload), and fourth (performance optimization of the network) phases of the TE process model defined in Section 3 of [1].

Incorporating survivability requirements into traffic engineering computations and the protection of traffic at different layers of the network is useful for a number of reasons:

(i) The most important is its ability to ensure stable network operation, which is a major consideration in real-time network performance optimization. A major challenge for Internet traffic engineering today is to ôexpect the unexpected.ö In other words, integrate automated control capabilities that can adapt quickly and at a reasonable cost to significant changes in network state, while maintaining network stability [1]. Clearly, this challenge cannot be met without accounting for potential network outages, and including them in - traffic engineering calculations.

(ii) Survivability considerations also impact the manner in which traffic is groomed at different layers (more on this in Sections 5 and 6), and the manner in which it is mapped to the underlying physical or logical topology at different layers of the network. An important function of TE is to control the distribution of traffic across the network, a task that is strongly influenced by the manner in which traffic is protected at different layers, and by how much traffic is protected at different network layers. An objective could be to provide adequate protection schemes at layer 0 that can classify and treat different traffic types, and dynamically assign the traffic to a specific protection scheme. This would ensure that, as much as possible, the higher layers need never know about the transport failures.

(iii) Yet another advantage is the ability to increase network reliability by enabling a faster response to faults and outages than is possible with a single layer alone (in particular, than is possible with Layer 3 or IP layer rerouting alone).

(iv) Protection at different layers gives the provider the flexibility to choose the granularity at which traffic is protected, and to also

choose the specific types of traffic that are protected.

(v) A protection mechanism at different layers (for example, the optical [3] and MPLS [8] layers) could enable IP traffic to be put directly over WDM optical channels, without an intervening SONET layer, thereby facilitating the construction of IP-over-WDM networks.

3. Purpose of This Document

The purpose of this document is to examine the survivability features and characteristics of different network layers, point out the advantages and limitations of each, consider how they impact network traffic engineering, and highlight service provider concerns and requirements and areas where further work may be needed, either in terms of independently extending the functionality of the existing layers or in terms of developing inter-layer coordination mechanisms to facilitate fast and efficient network protection. The document is intended to expose those areas pertaining to network survivability that require further work by the Internet community, and to serve as a basis for the Traffic Engineering Working Group design team to make recommendations to other Working Groups about network survivability issues that require further consideration in the respective Working Groups.

4.Motivation

The need for network survivability and for open standards in protection/restoration at different network layers arises because of the following:

-- Lower layer mechanisms (Optical Layer and SONET/SDH Layer) have no visibility into higher layer operations (for example protocol errors, priority identification, and reroute calculation). Thus, while they may provide link protection for example, they cannot easily provide node protection unless these optical devices speak the same ôlanguageö.

-- Optical Layer or SONET/SDH Layer mechanisms may initially be limited to ring topologies and may not always include mesh protection.

-- MPLS/ATM Layer may provide protocol-level node survivability, but may not be able to detect physical layer impairments.

-- IP Layer rerouting may be too slow for a core IP network that needs to support time-sensitive applications. Fault isolation is more difficult at the IP Layer than at the optical or SONET/SDH Layers.

-- Higher layer mechanisms (TCP, UDP, OSPF, and BGP) have limited visibility into lower layer operations (for example, into the optical and SONET/SDH layer physical failures).

-- Establishing interoperability of recovery/protection mechanisms between multi-vendor equipment in core IP networks is urgently required to enable adoption of IP as a viable core transport technology and to facilitate the traffic engineering of future multi-service IP networks.

5. Network Survivability Objectives

It is useful at this point to consider some of the objectives for network survivability. We propose the following generic objectives for network survivability.

5.1 Survivability Mechanisms

Network survivability mechanisms SHOULD:

-- Maximize network reliability and availability.
-- Facilitate fast recovery times where appropriate.
-- Take into consideration the recovery actions of different layers. For instance, if lower layer mechanisms are utilized in conjunction with higher layer survivability mechanisms, the lower layers should have an opportunity to restore traffic before the higher layers do. If lower layer restoration is slower than higher layer restoration, the lower layer may communicate failure information to the higher layer(s), and allow it to perform recovery. The coordination functionality between layers must be tunable.
-- Avoid network layering violations. That is, defects at higher layer(s) should not normally trigger recovery actions at lower layers.
-- Minimize the loss of data and packet reordering during recovery operations.
-- Minimize the additive latency that may be incurred when recovery is activated.
-- Minimize the state overhead of maintaining recovery information (such as additional paths, the association between traffic streams and paths, the association between what traffic is protected at which layers, and so on).
-- Allow other (e.g., low priority) traffic access to the protection bandwidth.
-- Be designed into the existing protocols to give as much flexibility as possible to the network operator.

In fact, the operator should have some alternatives to choose from when deciding what type of protection to implement. The most logical way to achieve this would be to use alternatives that are realizable by using the mechanisms currently defined for each layer. Basically, there could be an option to have different schemes of protection operate in a graded manner. For example, schemes like ring protection for the first 50 ms, and if that is not enough backup to mesh restoration. Another useful capability could be the ability to define different protection schemes per class of traffic.

The next few sections discuss some of these alternatives.

5.2. Survivability Actions

Network survivability actions SHOULD:

-- Not adversely affect other network operations.
-- Not adversely affect recovery actions at a different layer.
-- Not adversely affect the survivability actions within different protection domain(s) within a given layer.
-- Not adversely affect performance levels, to enable adherence to SLAs.

5.3. Survivability Techniques

Network survivability techniques SHOULD:
-- Be specifiable for dedicated or shared protection of working traffic.
-- Be specifiable on an end-to-end basis or on a segment basis. (For example, at the ATM , MPLS, or IP layer survivability should be specifiable for an end-to-end path or for a segment of a path.)
-- Be specifiable for protection of traffic at different granularities (for example, temporal, bandwidth, and QoS granularities; more on this in Section 6).
-- Be specifiable for protection of traffic having different transmission and/or preemption priorities.
-- Be able to fallback on different protection schemes, should the primary scheme be unavailable.
-- Be able to maintain BGP state (where appropriate), if at all possible.
-- Not allow the provisioning of additional traffic if the survivability constraints of the existing traffic get violated by admitting additional traffic.

6. Network Survivability: Parameter Considerations

In this section, we focus on considerations that affect the choice of the recovery scheme, and also the specific layer(s) at which network providers may choose to perform recovery.

6.1. Time-scale of Operations

The time-scale of the recovery operation is an important factor in determining which layer to perform network survivability. In a generic sense, the closer to the fault the faster the recovery. However, faults occur at different layers and not all layers have visibility to all faults at the different layers. The time-scale of recovery operations must be considered when choosing the network survivability mechanism(s).

6.2. Resource Efficiency

The efficient use of the network resources varies from one layer to the next. The resource efficiency of recovery operations must be considered when choosing the network survivability mechanism(s).

6.3. Signaling Mechanisms

In order to perform end-to-end and segment recovery operations, there has to exist a signaling mechanism to notify the network recovery operation. Some layers have this capability inherently (for example IP Layer), others (for example optical layer) -may not. (Although recently there have been proposals that integrate the optical layer with Layer 3 routing and that allow, for example, BGP updates to be triggered upon the detection of a fault at the optical layer.) The signaling mechanisms initiate the recovery operations and must be considered when choosing the network survivability mechanism.

6.4. Recovery Granularity

The recovery granularity of the different layer recovery operations should be a key requirement in network survivability. In a generic sense, the higher the layer, the finer the granularity. The Optical and SONET Layers can only recover full pipes (i.e. OC48 Granularity), whereas IP Layers can recover individual packets or groups of packets. The recovery granularity must be considered when choosing the network survivability mechanism. It is conceivable that the more granularity at the optical layer the better it may be for recovery. However, the granularity at the sub-wavelength level would work only with OEO devices and not with all-optical ones. Furthermore, the optical layer still may not provide recovery on a per-connection basis (unless the ôconnectionö was an entire wavelength or an entire sub-channel that the optical layer understands.)

6.5 QoS Granularity

The QoS granularity is a key requirement for traffic engineering and therefore for recovery operations. The QoS granularity must be considered when choosing the network survivability mechanism. It is to be noted that optical switches that are able to prioritize wavelengths might allow for traffic to be mapped to a priority scheme, which in turn is mapped to wavelengths with differing priorities, thereby providing some QoS granularity.

6.6. Coverage

The coverage desired by the recovery operation must be defined. Each layer provides adequate coverage for that layer, but perhaps not adequate coverage of the other layers. To provide more optimal coverage of the layers, interworking of recovery mechanisms between two or more layers should be considered. For example, combining the Optical Layer fast detection of a link layer failure with notification to the IP layer that rerouting must occur will provide coverage of both the Optical Layer and the IP Layer. The recovery coverage must be considered when choosing the network survivability mechanism.

6.7. Fault Monitoring/Reporting

The key aspect of recovery operations is the ability to detect faults. It is important to understand the various faults that each layer can detect, the fault monitoring capabilities and the fault reporting mechanism. The fault monitoring and reporting mechanisms must be considered when choosing the network survivability mechanism. The reports may include not only the failed/unplaced circuits, but also information on circuits that were placed/routed but have violated their performance or QoS constraints.

6.8. Interlayer Considerations/Layer Interactions

As previously mentioned in the coverage considerations, there are many advantages to providing a recovery mechanism that interoperates across one or more layers. Any such mechanism must not violate any one-layer recovery operations or cause another layer to incorrectly recover due to

a different layer operation. The consideration for providing layer interactions between the different layers is discussed in the next section.

7. Network Survivability: Layer Considerations

In this Section we focus on the specifics of the different layers in the light of the discussions in the previous Section. We enumerate the pros and cons of undertaking network protection/restoration at each of these layers, and consider the issue of systematically coordinating the actions of these layers to achieve enhanced network survivability and improved network operation.

7.1. Optical Layer

The optical layer is increasingly becoming the de facto physical layer in most core transport networks. With the advent of DWDM technology, the optical layer is now capable of providing very high bandwidth pipes (on the order of a 100 wavelengths per fiber, each operating at up to 10 Gb/s) that can be routed over large WANs or backbone networks to provide extremely high data rate connectivity between smaller, geographically dispersed networks.

The advantages of the optical layer are:

(i) Fast fault/failure detection: the loss of light or carrier signal at the optical layer can be detected quickly by the end node equipment. Thus, end points of a link, and, in some cases, lightpaths (such as when there is 1+1 protection), can detect link failure within a relatively short period of time (a few milliseconds)[9], and can switch to a backup lightpath, if configured.

(ii) Large switching granularity: the optical layer has the capacity to restore very large numbers of higher layer flows. For example, hundreds of LSPs or ATM VCs that would ordinarily be affected by a single link failure (such as a fiber cut) could be restored simultaneously at the optical layer without the need to invoke higher layer signaling, which can be computationally expensive and slow (since it may require processing by intermediate nodes, and must invariably encounter propagation delay).

Some current limitations of the optical layer are:

(i) Limited range of granularity: The optical layer can only restore the traffic at lightpath or sub-lightpath granularity, and is therefore suitable when all the data on a lightpath or sub-lightpath requires protection/restoration. It cannot restore individual circuits or paths.

(ii) No discrimination between different traffic types: The optical layer being bit-transparent is oblivious to actual traffic content on a lightpath and cannot, in general, differentiate between different traffic types. We note that some discrimination may be possible based purely on the physical and transmission properties of the lightpaths concerned, such as loss, dispersion, jitter, crosstalk, etc. The physical and transmission properties of the lightpaths provide a way to discriminate between the quality of the lightpaths themselves, and may not necessarily translate into higher layer QoS goals.

(iii) The speed of detection is dependent on the locality of the switching action. The speed advantage of the optical layer comes from its ability to detect the absence of light, and perform ôlocal repairö by mending the connection at the point of failure. However, if the

detection point and switching point are distinct, as may be the case in shared path protection (as opposed to 1+1 path protection), the desired and the protection switching point might be the origin of the lightpath. If this is the case, some form of signaling between optical equipment will be necessary [3]. In such situations, the response time of the optical layer will be dependent on the signaling mechanism deployed. Indeed, a deficiency of the current optical layer is its inability to signal failure notification, and the absence of an automated mechanism to perform protection switching in the general (the non 1+1) case. There are some schemes that propose to integrate optical layer detection with layer 3 signalling, by allowing routing updates to be distributed immediately following the detection of a fault at the optical layer. This could speed up recovery considerably, since it triggers higher layers rerouting decisions much quicker than they would be ordinarily.

7.1.1 Considerations for the Optical Layer

A consideration for the optical layer would be to provide some coordination between the optical layer detection and a higher layer that has a signaling mechanism, as is proposed, for example, in [3], [4], [11]. This would increase the flexibility at the optical layer by speeding up and expanding its rerouting capability and facilitate the deployment of newer, bandwidth efficient protection options, such as shared mesh protection.

Another consideration for the optical layer is that it cannot, in general, detect faults in the router or switching node, and so may not be able to provide true path protection at the LSP or ATM VC level, since faults in the switching equipment would not be detected by the optical layer. It is conceivable, in this case, that the reverse of the process described above could be used. Namely, if there was communication between the routing/switching equipment and the optical equipment, the optical layer on learning of a router/switch failure (it would still not detect faults at higher layers due to misconfiguration of the switching equipment), could initiate protection at the optical layer (by causing an deliberate loss of light condition).

Appropriate grooming of traffic on to a lightpath must be another consideration at the optical layer that would impact traffic engineering and network planning. The grooming algorithms, which traditionally are geared to most efficiently pack higher layer traffic onto a lightpath, would need to be modified to now take traffic protection or QoS needs into account, and groom like traffic (for example, traffic that requires a high degree of survivability) onto a small number of wavelengths that can be protection switched to meet SLA objectives. At the same time, the algorithms should also be able to pack best-effort (or low priority) traffic on to protection bandwidth pipes or 1+1 protection paths, thereby making the grooming of ôbumpable trafficö an important consideration as well.

7.2. SONET Layer

The SONET layer is the medium of choice in a large base of existing network infrastructures. While some of the considerations here are similar to those at the optical layer, the SONET layer currently offers more flexibility than a pure optical layer.

Some of the advantages of the SONET layer are:

(i) SONET protection is standardized and can operate across domains.

(ii) The SONET layer provides both detection and automatic protection switching.

(iii) The SONET layer provides greater control over the granularity of the channels that can be protection switched.

Some of the current limitations of the SONET layer are:

(i) Inefficient use of spare capacity: SONET protection is largely limited to ring topologies, where spare capacity often remains idle, making the efficiency of bandwidth usage an issue.

(ii) Limited topological scope: SONET protection is largely limited to ring topologies, which reduces the flexibility to deploy somewhat more complex, but potentially more efficient, mesh-based restoration schemes.

(iii) Lack of traffic priority: As with the optical layer, the SONET layer also cannot distinguish between different priorities of traffic. For example, it is not possible in SONET to switch EF (expedited forwarding) and AF (assured forwarding) streams based on priority.

(iv) Oblivious to higher layer failure: Like the optical layer, the SONET layer too is oblivious to higher layer errors or faults. Thus, SONET cannot detect ATM (or MPLS) layer errors. For instance, a corruption of packets at the ATM layer will not be detected by SONET processing.

7.2.1 Considerations for the SONET Layer

As with the optical layer, an important area of consideration at the SONET layer, from a TE perspective, is also one of traffic grooming. When network survivability must be taken into consideration, the grooming of traffic may need to be done not only for maximum efficiency, but also for maximum efficiency given that protection will be needed (and that traffic may require different types and extents of protection). A related issue is one of appropriately mapping the groomed channels to optical lightpaths, while keeping protection constraints in mind.

7.3. ATM Layer and/or MPLS Layer

In this version of this draft we will consider the ATM and MPLS layer together, since many of the issues that are involved are common to both.

Before proceeding further, however, it is essential to clarify the use of the term ôMPLS Layerö in this document. MPLS merely combines Layer 2 forwarding (label swapping) with Layer 3 (IP) routing, and does not, strictly speaking, satisfy the criteria for being an independent layer (it does not, for example, have any layer specific address). We use the term ôMPLS Layerö here to refer to the software and hardware that together implement MPLS signaling and forwarding functionality, but do not include the IP layer and its associated routing software in the ôMPLS Layer.ö

Some of the advantages of the ATM or MPLS layer are the following:

(i) Capability to detect router/switch faults: Both the ATM and

MPLS layer provide the capability to detect û faults in the router or switch, which are invisible to lower layers. For example, the SONET or the optical layer may not be able to detect faults that arise from the failure on a router/switch (such as the failure of the control card of the router/switch resulting in corrupted ATM or MPLS control packets), which can be detected by the ATM or MPLS layer. The ATM layer can do so via the F1-F5 errors and via its peering capability, whereas the MPLS layer may do so via an appropriately implemented liveness message (for example, the LDP Liveness message).

(ii) Capability to detect misconfigurations: Both the ATM and MPLS layer can detect node or software misconfiguration by the counting of errored or corrupted packets, which may be identified by looking at the ATM header or MPLS label. In ATM, this may involve tracking VPI/VCI mismatches, while in MPLS this may be accomplished by counting TTL errors or label mismatches

Other advantages of the ATM layer are the existence of an in-band OAM functionality that can help to detect path errors along a virtual circuit or virtual path, and also provides faster detection and restoration than is possible by relying on routing protocols alone.

Some of the current limitations of the MPLS layer are:

(i) (i)Difficulty of detecting physical link failures: The MPLS layer cannot detect failures without an explicit mechanism like a path continuity test [9] or a fast liveness message test [10]. Since MPLS does not allow for in-band signaling or OAM functionality of the type provided by ATM, an issue here is the ability to ensure that the liveness message can follow the exact path followed by an MPLS LSP between two LSRs.

(ii) The MPLS header is to small to allow for OAM functionality of fault and performance management.

7.3.1 Considerations for the ATM and/or MPLS Layer

As discussed, fault detection at the MPLS layer could be by detecting TTL errors or by counting unlabeled packets or packets with unrecognized labels. An issue with TTL errors is that they could be the result of either an MPLS layer or an IP layer problem, since the MPLS header carries the IP TTL. For instance, TTL mismatches could be due to a genuine problem with an upstream LSR or due to a router upstream of the LSR detecting the mismatches, probably the edge router that converted the IP packet into a labeled MPLS packet. Likewise, the persistent receipt of unlabeled packets or packets with unknown labels might indicate protocol problems, and necessitate a protection switch. Thus, detection of some types of errors at the MPLS layer may require a protection switch at the same layer, which is independent of lower layers.

7.4 IP Layer

The IP layer is central to the IP network infrastructure. Some of the advantages of the IP layer for survivability include:

(i) The ability to find optimal routes: The IP layer runs routing algorithms that can be tuned to propagate information that facilitates the calculation of optimal routes through the network, and perform constraint-based routing [10]

(ii) Better granularity of protection: Clearly, at the IP layer one obtains a fine level of granularity at which protection can be done. This layer allows a path selection algorithm to pick paths based on priority and other requirements of the traffic.

(iii) Load balancing ability: At the IP layer, one has the maximum flexibility to perform load sharing by distributing traffic across different paths (for example, by hashing using the source and destination address), and the flexibility to select a better path if it becomes available.

Some of the drawbacks of the IP layer in terms of survivability are:

(i) A well-known drawback of the IP layer, of course, is that recovery operations here can be quite slow relative to the lower layers. Connectionless recovery, due to its dependence on IP routing, can take seconds to detect loss of connectivity (via routing protocols) thereby slowing down the recovery action.

(ii) Another problem with the IP layer is that it too cannot detect physical layer faults, in that the IP layer may only be aware of the existence of a fault (through the non-receipt hello or keepalive messages in routing protocols), but may not know where the fault is. Thus, if the intent is not to always rely on fault recovery based on IP rerouting fault isolation may be an issue.

7.4.1 Considerations for the IP Layer

One of the major considerations for the IP layer is the time to detect faults. In IP connectionless networks, faults affecting TCP sessions for example can take a long time to detect since the end-systems must decide whether or not a session was lost. Thus, in order for the IP layer to provide reliable operation and fast recovery it has to work in conjunction with a path pinning mechanism (such as MPLS).

7.5. Transport Layers

The Transport layers are central to the IP network infrastructure. Some of the advantages of the Transport layers for survivability include:

(i) The ability to provide positive acknowledgement with retransmission (ACK).

(ii) The finest granularity of protection-application level: Clearly, at the TCP layer one obtains a fine level of granularity at which protection can be done. This layer allows a path selection algorithm to pick paths based on priority and other requirements of the application.

Some of the drawbacks of the Transport layers in terms of survivability are:

(iii) A well-known drawback of the Transport layer, of course, is that recovery operations here are quite slow relative to the lower layers. Connectionless recovery, due to its dependence on IP routing, can take seconds to detect loss of connectivity (via ACKS and sequence violations (TCP) or routing protocol (UDP)) thereby slowing down the recovery

action.

(iv) Another problem with the Transport layer is that it too cannot detect physical layer faults, and fault isolation may be an issue if the intent is not to always rely on fault recovery based on IP rerouting.

7.4.1 Considerations for the Transport Layer

One of the major considerations for the Transport layer is the time to detect faults. In IP connectionless networks, faults affecting TCP sessions for example can take a long time to detect since the end-systems must decide whether or not a session was lost. Thus, in order for the Transport layers to provide reliable operation and fast recovery it has to work in conjunction with a path pinning mechanism (such as MPLS).

7.6 Coordination between Layers

As mentioned throughout this document, the coordination of the recovery actions across layers could dramatically improve the response times of the network to faults, and would be valuable in designing and managing traffic engineering mechanisms to better optimize network performance. Even though each layerÆs fault detection mechanisms must be independent, as explained in the preceding sections, the ability to collapse the independent layers in a manageable and constrained manner will be important. In particular, the interworking of failure indications across layers to speedup recovery operations at higher layers.

An example of a higher layer failure that would not be detected at a lower layer is corruption of a packet at the ATM or MPLS layer, but not at the SONET layer. Thus, SONET processing would not be able to detect such a fault, and this would have to be recovered at the higher layer. By contrast, a fiber cut or link impairment is an example of a lower layer fault that is not visible at the higher layer, so the ability to communicate such fault information across layers may enable a lower layer, such as the optical layer, to take advantage of finer-scale protection capabilities of the higher layers by enabling them much quicker than they normally would. Some major impacts that designing coordination between the different layers is how to efficiently design the network with high reliability and availability. Additionally, the nature of SLAs that a provider could sign with customers will provide another degree of design considerations.

8. Service Provider Considerations

This section provides an overview of some aspects related to network survivability that service providers may consider when defining their requirements. Our objective here is to lay down some initial thoughts, and solicit feedback from individuals in the service provider arena.

-- Understanding how important network survivability is to the service provider organization

. Service providers might place different degrees of importance on survivability depending on the nature and type of traffic conveyed. It would, therefore, be important to know the relative importance of survivability for different services offered.

-- Defining the survivability adequacy of the following:
  a. DWDM
  b. SONET APS
  c. SONET UPSR
  d. SONET BLSR
  e. MPLS
  f. ATM
  g. IP
  h. Other

It is also necessary to assess the importance of survivability at different layers, and the most common layer at which survivability is currently provided.

-- Describing the areas that service providers would either require additional survivability functionality, or, if additional functionality was added to a specific layer, would change their opinion about providing survivability at that layer.

-- Determination of whether multi-layer survivability is required/desired, and specifying the extent and scope of such survivability.

For instance, if SONET detects a LOF should it provide a notification to MPLS layer to perform restoration? The point being that MPLS would have insight to the TE requirements of the operator environment (through policies for example), and could therefore find a more optimal route. Or is it that each layer should only provide survivability for itself and leave survivability of other layers to mechanisms within those layers.

-- Collect service provider survivability strategies, performance objectives, and requirements to identify framework level requirements on survivability.

-- Define the switch-over time objectives, granularity of traffic that must be supported, and scope (end-to-end, segment, node, link, combinations) of survivability strategies.

-- Identify the extent to which excess traffic would be utilized on backup paths during normal operating conditions.

9. Security Considerations

This document raises no new security issues for any of the protocols discussed herein.

10. Acknowledgements

The authors thank Kwabena Akufo for bringing the authors of this draft together, Dan Awduche for initial suggestions and hints regarding the subject matter of this draft, and Loa Andersson for highlighting the need to clarify the meaning of the phrase ôMPLS layerö as used in this document.

11. References
11. AuthorsÆ Addresses

Ken Owens
Erlang Technology, Inc.
1106 Fourth Street

St. Louis, MO 63126

Phone: 314-918-1579
keno@erlangtech.com

Vishal Sharma
Metanoia, Inc.
335 Elan Village Lane, Unit 203

San Jose, CA 95134-2539
Phone: 408-943-1794
v.sharma@ieee.org

Mathew Oommen
Williams Communications
One Williams Center
Tulsa, OK 74172-2067
Phone: 918-547-3043
Mathew.Oommen@wilcom.com

Full Copyright Statement

---

[1] Awduche, D. et al,"Framework for Internet Traffic Engineering," Work in Progress, Internet Draft, Work in Progress, draft-te-framework-05.txt, June 2001.
1 Ken, the original passive voice sounded better to me here.
[2] Kompella, K. et al, "OSPF Extensions in Support of Generalized MPLS,ö Internet Draft, Work in Progress, draft-kompella-ospf-gmpls-extensions-01.txt, February 2001.
[3] Rajagopalan, B., et al, "IP over Optical Networks: A Framework,", Work in Progress, draft-ietf-ipo-framework-00.txt
, July 2001.
[4] Lang. J., et al, "Link Management Protocol for Optical Networks," Work in Progress, Internet Draft, Work in Progress, draft-ietf-mpls-lmp-02.txt, April 2001.
[5] Awduche, D. O., Rekhter, Y., Drake, J., Coltun, R., ôMulti-Protocol Lambda Switching: Combining MPLS Traffic Engineering Control With

Optical Crossconnects,ö Internet Draft, Work in Progress, draft-awduche-mpls-te-optical-03.txt, May 2001.
[6]Ashwood-Smith, P., Berger. L. (Editors), "Generalized MPLS Signaling Functional Description", draft-ietf-mpls-generalized signaling-04.txt, Internet Draft, Work in Progress, May 2001
[7]Sharma, V., Hellstrand, F. (Editors) "A Framework for MPLS-based Recovery," Work in Progress, Internet Draft, draft-ietf-mpls-recovery-frmwrk-03.txt, July 2001.
[8] Owens, K., , Sharma, V., Makam, V., Mack-Crane, B., and Huang, C., "A Path Protection/Restoration Mechanism for MPLS Networks," Work in Progress, Internet Draft, draft-chang-mpls-path-protection-03.txt, July 2001.
[9] Shew, S. "Fast Restoration of MPLS Label Switched Paths," Work in Progress, Internet Draft, draft-shew-lsp-restoration-00.txt, October 1999.
[10] D. Awduche, "MPLS and Traffic Engineering in IP Networks," IEEE Communications Magazine, December 1999.