Emerging Technologies for Fiber Network Survivability

Reducing network protection costs, while maintaining an acceptable level of survivability, has become an important challenge for network planners and engineers. Technology advancement is certainly crucial for meeting this challenge, especially in the future B-ISDN environment.

Tsong-Ho Wu

Network survivability is an issue of great concern to a telecommunications industry eager to deploy high-capacity fiber networks [1-4], since loss of services in high-capacity fiber systems due to disasters and catastrophic failures could be devastating and result in significant revenue loss. However, providing protection against fiber network failures could be very expensive due to the high costs associated with fiber transmission equipment. Thus, reducing network protection costs while maintaining an acceptable level of survivability has become an important challenge for network planners and engineers. Technology advancement is certainly crucial for meeting this challenge, especially in the future B-ISDN environment. Technologies of interest for fiber network survivability include Synchronous Optical Network (SONET), Asynchronous Transfer Mode (ATM), and passive optical technologies (including optical switching and Wavelength Division Multiplexing (WDM)). These technologies provide the network protection technology base for each layer of the B-ISDN transport network defined in CCITT Rec. 321: physical layer (SONET in North America), ATM layer, and a possible optical layer, as shown in Fig. 1.

This article will review technology and architectures that may be used to implement cost-effective survivable fiber networks for each transport layer, and discuss the interworking system between survivability mechanisms across different layers and associated open issues. Standards development, product availability and the current status of deployment will also be reviewed.

The first section reviews a class of survivable fiber network architectures that has been deployed or is scheduled to be deployed. Next is a review of emerging technologies for these survivable architecture implementations. These emerging technologies include SONET, ATM, and passive optical technology. The next section discusses the issue of multiple layer interworking on SONET/ATM networks. A summary is given in the final section.

A Class of Survivable Network Architectures

The fiber-hubbed architecture has been considered as an economical transport architecture for intralATA networks. This architecture can best utilize the economical scale of high-capacity fiber systems by reducing the amount of expensive fiber terminating equipment needed. In this architecture, each central office (CO) is connected to a hub through a fiber-optic system. At the hub, a digital cross-connect system (DCS) partitions incoming traffic by destination and routes channels, over fiber, to the appropriate end office. Aggregating interoffice traffic onto a single fiber pair greatly reduces the costs for small COs that require links to other offices. The fiber-hubbed architecture is economically attractive, but at the expense of service vulnerability, since a single fiber cut or a hub office failure would isolate a large area served by the failed facility or CO from communicating with other communities.

To alleviate survivability concerns caused by the fiber-hubbed network architecture, several modifications to the hub architecture and alternative survivable architectures have been explored in the past few years. These survivable architectures include automatic protection switching (APS) with diverse protection (APS/DP), self-healing rings (SHRs), and dynamically path rearrangeable mesh architecture. Some proposals (e.g., APS and rings) have already been implemented and deployed in local exchange carrier (LEC) networks.

These survivable network architectures are generally divided into two categories: dedicated facility restoration and dynamic facility restoration. Dedicated facility restoration uses the dedicated protection facility for service restoration, while dynamic facility restoration uses the spare capacity within working facilities for service restoration. The former restoration category includes APS and rings, while the latter includes dynamic path rearrangeable mesh architecture and dual homing. There are tradeoffs between the flexibility (thus, system complexity) and the additional spare
capacity required for each restoration category. In general, the more sophisticated techniques require less spare capacity but slow down the restoration procedure. Figure 2 depicts four survivable network architectures which are described next.

**APS Diverse Protection (APS/DP)**

The APS approach shown in Fig. 2(a) has the advantage of being totally automatic and is commonly used to facilitate maintenance and protect working services. The 1:N diverse protection structure is an alternative to the commonly used 1:N protection structure, where N working fiber systems share one common protection fiber system. The only difference between these two structures is the location of the fiber protection system. The 1:N protection structure places the protection fiber in the same route as that of working systems, and the 1:N diverse protection structure places the protection fiber in a physically diverse route. In a 1:N system, a cable cut may cut the protection fiber as well as the working fibers. If a fiber cable cut occurs and a 1:N diverse protection scheme is used, part of service can survive because one of the N working systems can be restored through the diversified, protected route. This diverse protection scheme is attractive in intralATA networks because electronics costs dominate total costs and remain unchanged when attempting to achieve higher survivability. A 1:1 diverse protection arrangement, which provides 100 percent survivability for fiber cable cuts, requires more facilities and equipment than the 1:N diverse protection arrangement.

**Dual Homing**

In contrast to the single-homing approach, which aggregates demands from a CO to destination COs through an associated home hub, "dual homing" is an office backup concept that assigns two hubs to each office and requires dual access to other offices. In the dual-homing approach, demand originating from a special CO is split between two hubs: a home hub and a designated foreign hub. In the case of a home hub failure, an office that uses dual homing can still access other offices through the backup hub. Fig. 2(b) shows such a dual-homing architecture. Dual homing does not automatically accomplish restoration by itself, but may be used in conjunction with DCNs that restore services at the path layer.

**Self-Healing Rings (SHRs)**

The SHR (see Fig. 2(c)), like the 1:1 diverse protection structure, is totally automatic and provides 100 percent restoration capability for a single fiber cable cut and equipment failure through its ring topology and simple, but fast, protection switching scheme. It can also provide some survivability for hub DCN failures or major hub failures (e.g., flooding or fires).

**Dynamic Path Rearrangeable Mesh Architecture**

The dynamic path rearrangeable mesh architecture uses DCNs to reroute demands around a failure point. Unlike APS/DP and rings, DCN restoration does not require standby protection facilities dedicated to working systems for restoration. Instead, it uses spare capacities within working systems to restore affected demands. Figure 2(d) shows an example of DCN restoration. In Fig. 2(d), demands between locations A and B are normally routed over a link between DCN#1 and DCN#2, but are rerouted through DCN#3 if a cable cut occurs on that link. A centralized or distributed control system may optimize the use of the available spare capacities by referring to a database that contains the status of the network (both working and spare capacities). The penalties for this efficient use of spare capacities, compared with other architectures, are the time and complexity needed for the controller(s) to communicate with the network DCNs, as well as maintenance of the database.

**Emerging Technology Impact on Survivable Fiber Network Architecture Implementation**

Since discussions of this section follow the concept of the B-ISDN transport model, it would be useful to define three network protection schemes (i.e., protection switching, rerouting and self-healing) here based on CCITT Rec. L131 [46].

**Protection switching** — Protection switching is the establishment of a pre-assigned replacement connection by means of equipment without the network management control function. The equipment may reside in either the connecting or terminating points of the related path level. An example of protection switching is APS and self-healing rings.

**Rerouting** — Rerouting is the establishment of a replacement connection by the network management control connection. When a connection failure occurs the replacement connection is routed depending on network resources available then. An example of rerouting is the centralized control DCN network restoration.

**Self-healing** — Self-healing is the establishment of a replacement connection by the network without the network management control function. When a connection failure occurs, the replacement connection is found by the network elements and rerouted depending on network resources available at that time. Examples of self-healing include the distributed control DCN network restoration.
The perceived advantages of the SONET ring in terms of costs, survivability, and control have made the SHR architecture a popular option in LEC networks. Restoration schemes use both re-routing and self-healing capabilities during network restoration.

SONET Protection Layer
SONET is a standard in North America that defines optical interface, rate, and format specifications for broadband optical signal transmissions [5]. SONET is designed to transport a wide variety of signal types with a basic signal format containing fixed overhead to support various “in-band” operations features. Network survivability is among some initial applications that were provided by SONET. For example, SONET technology, along with high-speed (e.g., 2.4-Gb/s) VLSI technology, makes add-drop self-healing rings practical and economical for use in intraLATA network applications [6].

SONET APS — The SONET APS protocol was initially proposed in 1986 and was standardized in ANSI T1X.1.5 in 1992 [7]. Two types of APS architectures (1:N APS and 1+1 APS) are defined in the SONET standard [7,8]. The 1:N APS architecture allows one of the N (permissible values for N are from 1 to 14) working channels to be bridged to a single protection channel. Unlike asynchronous APS systems that use out-band signaling, the SONET APS protocol uses in-band signaling for protection switching through K1 and K2 bytes within the SONET line overhead. The K1 byte requests a channel for the switch action, and the K2 byte confirms the channel that is bridged onto the protection line.

The SONET APS protocol uses a three-phase protocol for bidirectional protection switching operations, which can be summarized as follows. When a failure is detected or a switch command is received at the tail end (i.e., the receiving end), the protection logic compares the priority of this new condition with the request priority of the working channel (if any) that requests the use of the protection channel. The comparison includes the priority of any bridge order (i.e., of a request on the received K1 byte). If the new request is of higher priority, the K1 byte is loaded with the request and the ID number of the channel requesting the use of the protection line. The tail end then sends out the K1 byte on the protection line.

When this new K1 byte has been verified (i.e., received identically for three successive frames) and evaluated (by the priority order) at the head end (i.e., the transmitting end), the K1 byte is sent back to the tail end with a reverse request (to confirm the channel requesting the use of the protection channel). A bridge is also ordered at the tail end for that channel. This action initiates a bidirectional switch. At the head end, the indicated channel is bridged to protection. When the channel is bridged, the K2 byte is set to indicate the number of the channel on protection.

At the tail end, when the channel number on the received K2 byte matches the number of the channel requesting the switch, that channel is selected for protection. This completes the switch to the protection channel for one direction. The tail end also performs the bridges, as ordered by the K1 byte and indicates the bridged channel on the K2 byte. The head end completes the bidirectional switch by selecting the channel from protection when it receives a matching K2 byte. Note that K1 and K2 bytes always travel over the protection line in present SONET standards [7]. Protection switching, including K1/K2 operations and switch reconfiguration, must be completed within 50 ms [8].

Another type of APS that is also defined in the SONET standard is 1+1 protection switching, which is a form of 1:1 APS with the head end permanently bridged. Thus, a decision to switch is made solely by the tail end. For bidirectional switching, the K1 byte is used to convey the signal condition to the other side, and the actual switching is decided by the tail end.

SONET Self-Healing Rings — In the past, the ring architecture has been restricted from interof-
office applications because these metallic, low-capacity systems may make the ring uneconomical and difficult to adapt to the rapidly growing traffic in the telecommunications interoffice network environment. Even in the present pre-SONET fiber world, the ring is used only in LANs, not in interoffice networks, because of its relatively low speed (approximately hundreds of Mbs), complex control scheme (as compared to the conventional facility protection switching architectures), and complex scheme to add-drop tributary signals from a high-speed signal. Recently, standardized SONET technology and associated flexible high-speed add-drop multiplexing technology (due to its synchronous frame format structure) have made SHR architectures practical because of SONET’s simpler control scheme, ease of adding-dropping tributary signals, and high-speed add-drop multiplexing capability (e.g., OC-48 with a bit rate of 2.488 Gbs), which may meet the intralATA interoffice demand requirement. The perceived advantages of the SONET ring in terms of costs, survivability, and simpler control have made the SHR architecture a popular option in the deployed of LEC networks. The first SONET self-healing ring was deployed by Cincinnati Bell in 1991, and operated at the OC-3 rate. Note that external controllers and the external telemetry system needed for asynchronous rings are not needed for the SONET ring because the failure message is conveyed and protection switching is triggered through the SONET line or path overhead.

SONET rings can be classified by the routing principle and the SONET overhead used for triggering protection switching [9]. A ring is called a unidirectional ring if bidirectional working signals follow opposite physical routes around a ring, while bidirectional working signals in a bidirectional ring follow the same physical route. Due to this routing principle, a unidirectional ring and a bidirectional ring require one fiber and two fibers, respectively, to support their working traffic. Each ring type can be protected through path protection switching operating at SONET pathlayer, line protection switching operating at the SONET line layer. Today, only unidirectional rings with path protection switching and bidirectional rings with line switching are defined in ANSI T1X1.5 and Bellcore requirements [10,11] and are commercially available in the U.S. market place. These ring types are currently under discussions in ITU-T Study Group 15 [12]. For convenience, a unidirectional set of rings (i.e., USHSRs) is mentioned in this paper is referred to as a unidirectional, path-switched ring. Similarly, a bidirectional self-healing ring (BSHR) mentioned here is referred to as a bidirectional, line-switched ring.

In a unidirectional path switched ring, two fibers are needed between adjacent nodes: one for working and the other for protection. A path (e.g., STS-1) in the transmitting side is duplicated and sent to both fibers in opposite directions. Thus the receiving end always receives two identical path signals with different delays. The receiving end always chooses a path from the default ring (e.g., the outer ring) but switches to the other ring if the ADM detects an alarm signal (e.g., path AIS) or a poor BER. The unidirectional, path switched ring may perform protection switching at the STS-1 or VT1.5 level depending upon applications.

Bidirectional self-healing rings (BSHRs) are further divided into 2-fiber and 4-fiber BSHRs. For a 4-fiber ring, two fibers are used for working traffic, while another two fibers serve as standby fibers that provides 1:1 protection against equipment or fiber facility failures. The 2-fiber BSHR uses only half the capacity of the fiber system for working traffic and reserves the other half as the protection capacity. To perform protection switching against network failures for a 2-fiber BSHR, a form of the Time Slot Interchange (TSI) capability is needed to move signals from time slots of the affected fiber to the reserved (spare) time slots of the other fiber. Note that standby fibers or capacities in BSHRs (as well as other 1:1 systems) are allowed to carry lower priority traffic that may be dropped during the network restoration process.

The application roles between USHRs and BSHRs have been extensively studied. It is generally agreed that a USHR may be more economically attractive in areas where demands are homed to one central location, while BSHRs may be attractive in areas where demands are more uniformly distributed [9]. This appears to imply that USHRs may be more appropriate in feeder networks and peripheral networks (e.g., from CO to the hub), and BSHRs may be more practical in interoffice networks with a non-hubbing structure. Thus, it is expected that different types of rings may be deployed in the same LATA network. This trend raises the issue of ring interworking, which is currently being discussed in the ANSI T1X1.2 standards group [13]. We will discuss this ring interworking issue later.

SONET self-healing rings were originally designed to support both voice services and private lines. However, the same ring structure has been implemented to support reliable transport for Cable TV signals. Figure 3 shows an example of the ring-to-ring broadcast architecture. If this broadcast ring architecture uses SONET technology, the SONET ADM at each node requires a drop-continue feature that drops signals for local processing and passes through the identical signals to the downstream node.

**SONET DCS Self-Healing Mesh Networks** — The operations of the DCS mesh network reconfiguration can be performed in a central or distributed manner. The centralized DCS control scheme has a central controller performing the network
reconfiguration process, whereas the distributed DCS control scheme executes the network reconfiguration procedure at each DCS node. Centralized DCS mesh restoration systems have been implemented by several LECs and long-distance carriers. The restoration speed is about 5 to 10 minutes for 100STS-1 (or DS3) paths restored. This restoration time can be significantly reduced by using the distributed control approach. The concept of distributed DCS restoration was first proposed by Grover in 1987, and was later modified and reported in [16]. This proposal uses the physical layer signaling. Another scheme was later proposed in [17] that uses section data communications channel (DCC) for signaling and a restoration protocol similar to the X.25 protocol. Later, several other schemes were proposed based on the above two proposals [18-23, 52].

There are two restoration techniques, called line restoration and path restoration, depending on which layer is being used as the protection layer. Line restoration uses the line layer information to trigger the restoration process and restores all affected paths in the affected facility regardless of the sources and destinations of these affected paths. In contrast, path restoration restores affected STS paths on an end-to-end basis. For the purpose of this paper, this section describes a generic line restoration algorithm for distributed control self-healing mesh networks. The restoration algorithm for path restoration is similar to that for line restoration. For the distributed self-healing control architecture, each DCS stores local information that includes working and spare capacities associated with each link terminating at that DCS. The actual implementation could vary depending on the specific algorithm considered. Due to dependence between the routing assignment and the capacity allocation in SONET DCS mesh networks, the distributed restoration system generally executes a three-phase protocol during a complete restoration cycle. When a failure is detected, one of two ends of the failed facility is designated as the sender, and the other end is designated as the chooser. All other nodes that participate in the restoration process are called tandem nodes. In the restoration process, the sender first broadcasts (floods) restoration messages to all adjacent nodes. To restrict the number of restoration messages and constrain the algorithm execution time, selective message flooding is implemented, for example, through limiting the number of hops that could be travelled for restoration messages. The tandem node updates received restoration messages and re-broadcasts them to other adjacent nodes based on the particular flooding algorithm used. When the message reaches the chooser, it implies that one or more rerouting paths for restoration are identified. The chooser then sends acknowledgment (ACK) messages back to the sender to reserve the spare capacity for the selected restoration route.

When the sender node receives the ACK, it verifies the restoration path, it sends a confirmation message back to the chooser node through the selected restoration path. When the tandem node receives the confirmation message, it reconfigures its DCS switching matrix according to instructions stored in the confirmation message. After the chooser receives the confirmation message, it changes its DCS switching matrix and cross-connects the affected STS paths from the failed facility to newly identified alternate routes. The restoration process is completed when all the affected paths are restored (provided that enough spare capacity exists). Note that reservation of DCS ports for the alternate routes can be made either in the first or second phases in each of the DCS nodes involved, whereas cross-connections are made in the last phase.

The viability of using the distributed control DCS self-healing mechanisms in intra-LATA networks in terms of economics, operations, and reliability was studied extensively by Bellcore in 1992, and study results have been summarized in [24]. This report verifies that the DCS self-healing network is economically attractive in areas where high demand and high connectivity are involved. Also, it is indicat-

<table>
<thead>
<tr>
<th>Attributes</th>
<th>APS/DP</th>
<th>SHR/ADM</th>
<th>DCS Mesh</th>
</tr>
</thead>
<tbody>
<tr>
<td>Network size</td>
<td>2 nodes</td>
<td>Up to few tens of nodes</td>
<td>Global</td>
</tr>
<tr>
<td>Spare capacity needed</td>
<td>Most</td>
<td>Moderate</td>
<td>Least</td>
</tr>
<tr>
<td>Per-node cost</td>
<td>Moderate (OLTM/APS)</td>
<td>Lowest (ADM)</td>
<td>Highest (DCS)</td>
</tr>
<tr>
<td>Fiber counts</td>
<td>Highest</td>
<td>Moderate</td>
<td>Moderate</td>
</tr>
<tr>
<td>Connectivity needed</td>
<td>Lowest</td>
<td>Moderate</td>
<td>Most (mesh)</td>
</tr>
<tr>
<td>Restoration time</td>
<td>- 50 ms</td>
<td>- 50 ms</td>
<td>Seconds/minutes</td>
</tr>
<tr>
<td>Mixed line rates</td>
<td>Possible for 1:N/APS</td>
<td>No</td>
<td>Yes</td>
</tr>
<tr>
<td>Software complexity</td>
<td>Least</td>
<td>Moderate</td>
<td>Most</td>
</tr>
<tr>
<td>Areas impacted by software failure</td>
<td>2 nodes</td>
<td>Nodes on the ring</td>
<td>Wider areas</td>
</tr>
<tr>
<td>Protection against major failure</td>
<td>Worst</td>
<td>Medium</td>
<td>Best</td>
</tr>
<tr>
<td>Scalability</td>
<td>Easiest</td>
<td>Most difficult</td>
<td>Moderate</td>
</tr>
<tr>
<td>Planning/operations complexity</td>
<td>Least</td>
<td>Moderate/least*</td>
<td>Most</td>
</tr>
</tbody>
</table>

* Assume that the USHR with path protection switching is used. Note that this comparison does not include the ring interconnection feature.

Table 1. Comparison of SONET survivable network architectures.
ed in [24,25] that currently proposed SONET distributed DCS restoration systems may not be able to completely restore services within two seconds in large metropolitan LATA networks, as long as the present DCS system architecture (i.e., serial processing and serial cross-connection) and its switching hardware technology remain unchanged. The network restoration time here includes the distributed control restoration algorithm (protocol) execution time and the DCS cross-connect time for network reconfiguration, where the DCS cross-connection time may be a dominant factor of the total restoration time in metropolitan LEC networks [24-25]. The slow cross-connection time of present DCS systems is primarily due to the inherent serial processing/cross-connect architecture and a slow cross-connection hardware system (e.g., about 100 ms-300 ms for each STS-1 path cross-connection).

To meet the two-second restoration objective, two basic requirements have been identified in [24, 25]. The first requirement is to design a DCS self-healing algorithm with a minimum set of restoration messages. The second requirement is to enhance the DCS performance by using a parallel CPU-based processing architecture with a parallel path cross-connection capability. Alternately, the two-second service restoration objective may be met by implementing priority service restoration. This restoration objective may also be relaxed based on hybrid network restoration architectures. These hybrid restoration architectures deploy fast restoration mechanisms (APS or rings) to meet specific customer needs on top of DCS mesh networks with distributed control that provide high survivability, enhanced protection against node failures and the adequate restoration time for most other customers. Which approach should be used depends on the cost for these system enhancement and the revenue expected from services supported by the distributed control DCS network restoration system. Also, it is suggested in [24] that using the SONET Section DCC channel for signaling will contribute several seconds to the restoration execution time just for its O91 protocol stack handling. Several alternatives for efficient signaling suggested in [24] include the use of the unassigned SONET overhead byte or out-of-band signaling such as DS0 or DS1.

**SONET Integrated Survivable Transport** — Table 1 shows relative comparisons among the SONET APS/DP, SHR, and DCS self-healing networks.

<table>
<thead>
<tr>
<th>Service</th>
<th>SONET APS/DP</th>
<th>SHR</th>
<th>DCS Self-healing</th>
</tr>
</thead>
<tbody>
<tr>
<td>Service Restoration</td>
<td>2 sec</td>
<td>2 sec</td>
<td>2 sec</td>
</tr>
<tr>
<td>Backup Path Provision</td>
<td>2 sec</td>
<td>2 sec</td>
<td>2 sec</td>
</tr>
<tr>
<td>Amplifier Cross-Connect</td>
<td>1 sec</td>
<td>1 sec</td>
<td>1 sec</td>
</tr>
<tr>
<td>Network Unavailability</td>
<td>0.1 sec</td>
<td>0.1 sec</td>
<td>0.1 sec</td>
</tr>
</tbody>
</table>

The APS/DP and rings have the similar capability to restore services very quickly (i.e., within 50 ms). Their major difference is in the growth impact and costs. Rings have a greater concern for system exhaustion, since all ADMs on the ring need to be upgraded in that situation. Thus, it makes APS/DP systems more appropriate in areas where point-to-point demand is extremely high, while rings are appropriate for areas where the growth rate is stable and relatively slow. Compared with the SHR, the DCS self-healing network requires less protection capacity, but requires longer restoration time and more complex planning and operations systems. The restoration time for the DCS self-healing network may range from seconds to minutes, whereas the restoration time for the SHR is within 50 ms. The spare capacity savings for the DCS self-healing network are primarily due to the sharing of spare capacities across the entire network. This sophisticated system provides tremendous advantages when it functions properly, but may cause problems in a much wider area (compared with APS and rings) when a software failure occurs. To avoid bringing the entire DCS network down due to software failures, sectionalization may need to be incorporated to improve the DCS network's reliability.

The differences among survivable architectures, summarized in Table 1, have resulted in a well accepted two-tier transport network model, as shown in Fig. 4. This two-tier transport network is composed of a core sub-network and a peripheral sub-network. The demand, network connectivity, and the network growth are primary factors for the two-tier network partition. The core sub-network, which favors DCS self-healing and/or high-speed APS/DP architectures, is a network having high connectivity, carrying high demand and a high growth rate. The peripheral sub-network, which favors rings and/or low-speed APS/DP, is usually deployed in areas where connectivity, demand and the growth rate are low. Examples of the core and peripheral subnetworks in today's fiber facility network are the hub-to-hub subnetwork (having either a star, hubbing structure with diversely protected routes or a ring structure), respectively.

**SONET Architecture Interworking** — As explained in the previous section, a network may use different types of survivable network architectures due to economics and demand distribution. Thus, how these different survivable network architectures interwork together becomes a crucial issue to ensure end-to-end service integrity during network failure conditions. The architecture interworking issues are currently under study in ANSI T1X1.2 [13]. The purpose of this study is to better understand the potential impact of ring interworking on various architectures (e.g., ring-to-ring, ring-to-DCS mesh), network interfaces and applications, and to provide recommendations on ring interconnection practices.

**Figure 4. A two-tier fiber transport network model.**

![Figure 4](image_url)

Figure 5 shows three ring interconnection within 50 ms. The spare capacity savings for the DCS self-healing network are primarily due to the sharing of spare capacities across the entire network. This sophisticated system provides tremendous advantages when it functions properly, but may cause problems in a much wider area (compared with APS and rings) when a software failure occurs. To avoid bringing the entire DCS network down due to software failures, sectionalization may need to be incorporated to improve the DCS network's reliability.

The differences among survivable architectures, summarized in Table 1, have resulted in a well accepted two-tier transport network model, as shown in Fig. 4. This two-tier transport network is composed of a core sub-network and a peripheral sub-network. The demand, network connectivity, and the network growth are primary factors for the two-tier network partition. The core sub-network, which favors DCS self-healing and/or high-speed APS/DP architectures, is a network having high connectivity, carrying high demand and a high growth rate. The peripheral sub-network, which favors rings and/or low-speed APS/DP, is usually deployed in areas where connectivity, demand and the growth rate are low. Examples of the core and peripheral subnetworks in today's fiber facility network are the hub-to-hub subnetwork (having either a star, hubbing structure with diversely protected routes or a ring structure), respectively.

**SONET Architecture Interworking** — As explained in the previous section, a network may use different types of survivable network architectures due to economics and demand distribution. Thus, how these different survivable network architectures interwork together becomes a crucial issue to ensure end-to-end service integrity during network failure conditions. The architecture interworking issues are currently under study in ANSI T1X1.2 [13]. The purpose of this study is to better understand the potential impact of ring interworking on various architectures (e.g., ring-to-ring, ring-to-DCS mesh), network interfaces and applications, and to provide recommendations on ring interconnection practices.

**Figure 5 shows three ring interconnection**
configurations defined in T1X1.2 [13]. Figure 5(a) shows an interworking configuration between two unidirectional path switched rings. In this configuration, the signal associated with interring traffic is dropped at one serving node and continued onto the second serving node using the drop and continue function. At both serving nodes, path selector functions choose independently the best of two incoming signals to drop into the next ring. Note that the path selectors can be set up to select the same path signal or set up opposite of each other as a default.

Figure 5(b) shows a configuration and a proposed method for interconnecting two bidirectional line switched rings. Similar to interconnected path switched rings, each ring uses a primary serving node and a secondary serving node for interconnection. The node at which the service would normally exit the ring is designated as the primary node and has an associated secondary node. This designation is made on a per service basis (e.g., STS-1). The service exiting the ring is dropped at the primary node and is also passed through the node (drop and continue) toward the secondary node. In the current proposed method, only primary nodes have service selectors that are required for interring traffic entering or being added to the bidirectional line switched ring. In the bidirectional ring, the service selector chooses between two copies of the service signal entering the ring at different points to determine which signal should be permitted to continue around the ring. If the service selector detects a signal failure on the primary signal, the service selector will "gang switch" to the appropriate signals coming from the secondary node. The secondary add signal is cross-connected toward the drop and continue (primary) node. Note that duplicate copies of the signal are dropped from the primary and secondary nodes of the ring. This allows interconnection between a unidirectional path switched ring and a bidirectional line switched ring, as shown in Fig. 5(c), without any changes to path switched ring requirements.

**ATM Protection Layer**

Restoration schemes at the ATM layer are still in the research and development stage. However, both ITU-T and ANSI/T1S1.5 have initiated some efforts to study ATM network protection issues. Since restoration systems currently deployed in LATA networks are performed at the SONET/SDH layer, it would be natural to ask why we need additional ATM layer protection systems. To understand the insight of this question, it is necessary to understand the difference between SONET/STM transport and SONET/ATM transport. One major difference between STM and ATM virtual path (VP) transport systems is in the path structure. STM transport uses a path structure that tightly links the physical connection and its capacity through TDM frames and their physical interfaces, while ATM/VP transport uses a logical path structure within which connections are linked to physical interfaces, but the connection capacity can be varied depending on applications. This path structure may simplify ATM/VP design and consequently increase link utilization, when compared with STM transport.

At the ATM layer, ATM cells can be transported and cross-connected either at the virtual channel (VC) layer or the VP layer, depending on applications, traffic patterns and the network size. As far as survivability is concerned, VP restoration is simpler and faster than VC restoration and has been a focus of ATM restoration systems currently proposed in the telecommunications industry [2]. Thus, the following discussions will primarily focus on VP restoration. The concept of VC restoration is similar to that for VP restoration. Unlike STM transport, for which the capacity
assignment is tied into the routing assignment, an ATM VP route is established by setting the routing table at VP connection points between VP corridor ends, and VP capacity is not explicitly assigned at the VP connection points at VP establishment due to its logical path structure. The capacity assignment of ATM VP transport is handled by separate management procedures, such as call admission control and usage monitoring, which are carried out at ingress connection end points. Thus, intermediate VP connection points on the VP route perform no processing for VP capacity management, and so are not affected by changes in the VP capacity allocation. The independence between the route assignment and the capacity allocation makes some ATM VP layer protection schemes more efficient and flexible than their STM counterparts.

**Protection Switching** — Protection switching at the ATM layer is an issue currently under study in ITU-T Study Group 13 and ANSI T1S1.5. The open technical issues associated with ATM layer protection switching include:

- Protection switching communication mechanisms (OAM cell, or ATM connections using AAL-5).
- Method of specifying a protection route (fragment end-to-end).
- Undirectional or bidirectional protection switching for point-to-point and point-to-multipoint systems (e.g., multicast video).
- 1:N, 1:1 and 1+1 protection switching.
- Inter-layer management for protection switching (SONET to ATM layer, including the protection control message exchange protocol and its protection scheme).
- "Hitless" protection switching system implementation and analysis.

Besides the technical issues listed above, application feasibility issues will have to be addressed before any practical ATM protection switching system can be realized. These application feasibility issues include: how ATM protection switching is different from today's SONET APS; and how ATM protection switching can best interwork with SONET APS. These two issues are equivalent to identifying appropriate application areas for both SONET/APS and ATM protection switching.

The OAM segment may include one or more VP links, where a VP link is a logical link between two adjacent VP cross-connect systems (VPXs) or VP ADMs. The second definition, called "line" definition, for protection switching fragmentation is the same as those used by SONET APS, where a fragment is defined as a VP link, if the VP layer is used as protection switching. In this case, AAL Type-5 may be a reasonable choice, since the end points of the fragment may not be an OAM segment, making it impossible for them to generate OAM cells for triggering protection switching. The last definition, called "general" definition, is to have a protection switching fragment use any arbitrary portion of the end-to-end connection for protection. Tradeoffs among these three possible definitions are summarized in Table 2 [49].

Although the signaling formats and protocols for protection switching at the ATM layer are still under discussion in the standards group, several hitless switching protocols have been proposed for in-service maintenance and protection switching in ATM VP-based transport networks [27, 28, 47, 49]. For facility maintenance, a VP must be moved from the original route to an alternate route without interrupting the cell stream on the original route. After maintenance is complete, the VP is switched back to the original route without service interruption. For VP protection switching, when the network component fails, the working VP is rerouted to the alternate route, and the VP will be switched back when the failed component is repaired. The reversion mode of protection switching allows the network to best utilize its resources as designed in the capacity provisioning phase.

The key factor that makes VP hitless switching possible is synchronization between the original route and the alternate route. The cell sequence integrity across VCs within a VP is also required for hitless path switching. In ATM networks, the synchronization signals can be inserted to replace the unassigned cells. Several synchronization methods for hitless path switching are proposed in [27, 28, 47, 49]. Among synchronization alternatives, snap-shot synchronization maybe the simplest one, although it requires buffers to adjust the difference of delays between the original and alternate routes if the original route is longer than the alternate route.

Note that if a VP link is a SONET link (i.e., no SONET equipment exists between two end points of the VP link), the switching control mechanism can use the existing SONET/SDH K1/K2 protocol [28, 47] to perform the protection switching.

---

**Table 2. Comparison of approaches for defining ATM protected fragment.**

<table>
<thead>
<tr>
<th>System factors</th>
<th>OAM approach</th>
<th>Line approach</th>
<th>General approach</th>
</tr>
</thead>
<tbody>
<tr>
<td>Protection switching unit</td>
<td>VP Line/VP</td>
<td>VP</td>
<td></td>
</tr>
<tr>
<td>Protection switching cell</td>
<td>OAM/AAL-5 AAL-5</td>
<td>AAL-5 AAL-5</td>
<td></td>
</tr>
<tr>
<td>Spare capacity needed</td>
<td>Moderate</td>
<td>Most</td>
<td>Less</td>
</tr>
<tr>
<td>Engineering complexity</td>
<td>Moderate</td>
<td>Least</td>
<td>Most</td>
</tr>
<tr>
<td>ATM node failure protection</td>
<td>Possible</td>
<td>No</td>
<td>Possible</td>
</tr>
<tr>
<td>Network design flexibility</td>
<td>Less</td>
<td>Less</td>
<td>Most</td>
</tr>
</tbody>
</table>

---

2 Note that if OAM cells are used to carry the protection switching message, two types of OAM cell formats are needed. One is associated with fault management's OAM cells designed for "hard" failures, and the other is associated with performance management's OAM cells for "soft" failures. This is because protection switching should be designed to recover the network from either "hard" failures (e.g., cable cuts) or "soft" failures (e.g., poor BER).
switching function. Several tradeoffs between SONET/SDH and ATM VP protection switching control mechanisms for ATM VP transport networks have been discussed in [49], and this is still an open issue requiring further study.

**ATM Self-Healing Rings** — SONET self-healing rings described earlier use STM technology for time slot allocation, and these time slots are dedicated to each node. As mentioned earlier, SONET rings are primarily designed to provide very fast (less than 50 ms) and cost-effective protection for private lines and voice services. However, when high-speed broadband data services and LAN interconnection services are gradually introduced into the network, STM ring transport starts to show its inability to handle these burst types of traffic efficiently. This is primarily caused by the STM transport’s hierarchical, physical path structure and its lower degree of flexibility in managing the bandwidth granularity. To alleviate this inefficient use of bandwidth for burst-type broadband services, bandwidth management schemes based on the ATM VC [29] and the VP layer [30, 31] have been proposed for working traffic bandwidth management. Although the bandwidth management schemes proposed above can be theoretically applied to both unidirectional and bidirectional rings, bidirectional rings may be preferred in terms of the minimum bandwidth allocation requirement due to a natural match between the inherent point-to-point VP characteristics and the point-to-point routing principle of bidirectional rings [4, 48].

Protection of ATM rings can be implemented at the SONET or ATM layer. SONET layer protection may use the SONET path layer for the unidirectional self-healing ring or the line layer for bidirectional self-healing rings, which is consistent with existing SONET standards defined in T1X.15 and Bellcore requirements [10, 11]. In the SONET path protection layer, either STS-3c, STS-12c or STS-48c protection may be possible, where STS-3c protection is primarily proposed for network evolution from existing SONET self-healing rings to ATM VP self-healing rings. Current Bellcore generic requirements for ATM VP rings using SONET layer protection focuses on bidirectional self-healing ring architectures because they require less spare capacities than their unidirectional counterpart [48].

If the VP layer is used for unidirectional ATM VP ring protection, the self-healing protocol as defined in the SONET path-switched self-healing ring [10] may be applied, except that the path selection is triggered by the VP-AIS (alarm indication signal), rather than the STS (or VT) AIS. Compared with SONET layer protection, VP layer protection may be more flexible and simpler. For example, assume that there are 20 STS-1s required for a node pair, it would require 20 STS-1 path splitters and selectors at each end node of that node pair for the SONET/STM path switched ring, but it would only need a VP splitter and selector for the VP at each end node of that node pair. However, the VP self-healing protocol needs to be standardized for the multi-vendor environment. Whether the SONET or VP layer should be used as the protection layer for ATM rings remains to be determined.

**ATM Self-Healing Mesh Networks** — As described earlier, the distributed SONET survivable mesh network architecture is considered as part of an integrated survivable transport network architecture. However, its inability of meeting a two-second service restoration objective in metropolitan LATA networks may make it impractical to support services requiring very fast restoration. This slow restoration time is due to its slow cross-connect time that functions as a dominant factor of the total restoration time. The slow cross-connect time of present DCS systems is primarily due to the inherent serial processing/cross-connect architecture and a slow cross-connection hardware system (e.g., about 100ms-300ms for each STS-1 path cross-connection).

ATM VP is a proposed concept that may significantly reduce the cross-connect time for network reconfiguration for distributed control mesh-type restoration systems due to its logical routing scheme on the self-routing switching fabric and its inherent parallel switching (cross-connection) capability. Independence between the alternate route selection and the capacity assignment for ATM VP networks may help simplify the design of the self-healing protocol, which makes the one-phase restoration protocol possible [27], compared with the three-phase restoration protocol used in SONET DCS distributed control networks. However, this one-phase ATM VP self-healing protocol may not provide the same reliability as its SONET DCS self-healing counterpart, unless the restoration message of the ATM one-phase protocol performed by ATM VP cross-connect systems (VPXs) is protected from transmission errors. The penalty for introducing link-by-link retransmission for restoration message protection is measured as approximately several ms per link [32], which may be insignificant compared with the total network restoration time. Also, the signaling channel using user information AAL-5 cells for restoration message exchange proposed in [32] has a much higher bandwidth for restoration message exchange, and more signaling cells can be generated within a time cycle of 125 ms than its SONET/STM counterpart. Furthermore, unlike the SONET DCS that can cross-connect with a single bit rate (e.g., STS-1), the ATM VPX may cross-connect VPXs with any bandwidth. This feature may make control and management of the ATM VP layer restoration easier and faster than in STM-based networks without penalizing bandwidth utilization for normal conditions.

Thus, the ATM VPX-based network architecture is a potential candidate architecture that may meet the two-second service restoration objective. Interested readers may refer to [2, 27, 50, 51] for details of some ATM self-healing algorithms.

**Optical Layer Protection**

Passive optical technology has been suggested as practical in reducing survivable fiber network costs [33]. The reason that passive optical technology is attractive as a network survivability option is a natural match between two major fast network protection requirements (i.e., minimum or no processing, and high capacity transport) and the basic characteristics of passive optical technology. Passive optical components of interest to network survivability include optical switching...
systems, wavelength division multiplexers, and optical amplifiers. The network using passive optical technology as the protection mechanism is sometimes referred to as a passive protected network [33].

**Passive Protected APS** — The automatic protection switching function of the diversely protected (DP) network architecture protects the network from fiber cable cuts, which is controlled by an automatic protection switching system (APS). In practice, point-to-point fiber systems with greater than the Gb/s capacity usually require 1:1 protection that may become very expensive, since it requires not only duplicate fiber facilities, but also terminating electronics equipment. For interLATA networks, the equipment cost is the dominant factor of total fiber transport costs. To reduce the protection cost, while retaining high survivability for cable cuts like 1:1/DP, a cost-effective 1:1 optical diverse protection (1:1/ODP) architecture was proposed in [34]. This architecture uses optical switches for 1:1 fiber cable protection and maintains 1:N electronic protection using a 1:N APS system. Figure 6 depicts an example of 1:1/ODP with N=3. In Fig 6, the 1:3 APS system protects three working terminals, and three diverse protection lines connected at the optical protection modules (OPMs). Each OPM includes a 50/50 power splitter (PS) on the transmit side and a 1 x 2 optical switch on the receive side. The PS splits an optical signal into both working and protection systems; the 1 x 2 optical switch, acting as a selector, switches demand from failed fibers to corresponding diverse protection fibers, when a cable containing working fiber pairs is cut. Assume that there are four 2.4 Gb/s 1:1/DP systems needed in the considered fiber span. The use of 1:1/ODP may reduce the protection cost of the conventional 1:1/DP system by up to 70 percent [34], although the 1:1/ODP system may be less survivable than the 1:1/DP system when two or more electronic components fail simultaneously. This type of passive protected APS systems is commercially available and is being deployed in some public carriers.

**Passive Protected Self-Healing Rings** — As described earlier, the SONET self-healing ring is viewed as a cost-effective survivable network architecture, and some ring architectures have been deployed in LEC networks. Among SONET self-healing ring alternatives, the four-fiber bidirectional self-healing ring (BSHR/4) has the largest available capacity and the highest reliability, and can work with today's operating system with minimum changes. The BSHR/4 is made up of one working ring with two fibers and one protection ring with another two standby fibers. However, the conventional BSHR/4 implementation requiring duplicated equipment (i.e., ADMs) in each node makes it relatively expensive compared with other self-healing ring alternatives. The BSHR/4 has been reported in [35].

Figure 7 depicts a generic BSHR4/PPR architecture for a ring network of seven nodes and its operations for a single link failure scenario. A BSHR4/PPR is composed of two parts: a SONET ring for bidirec-
A desirable characteristic of optical amplifiers used in the BSHR4/PPR is that they should be able to accept a large variation of input power and provide a near constant output powers.

A directional working signals, and a totally passive protection ring for bidirectional protection signals. One SONET ADM is required for each working ring node to carry bidirectional traffic. The protection ring is composed of optical switches, as well as optical amplifiers if the ring size is large. The passive protection ring is essentially an optical add-drop protection ring, where optical switches at the two ends of the failed facility act as optical "add-drop" components, and optical switches at intermediate ring nodes act as optical "pass-through" components. The optical signal add-drop is controlled by SONET ADMs on the working ring. The high-speed loopback function is performed through 1 x 2 and 2 x 2 optical switches. Optical protection switches eliminate the need for duplicated ADMs. One or more optical amplifiers, which are optional components of the BSHR4/PPR, may be needed for optical signal amplification if the protection ring is large. Although the optical amplifier(s) is placed in the ring topology, it does not form an optical signal amplification ring (loop), since the optical signal carried on the protection ring is added and dropped at two different optical switches. A desirable characteristic of optical amplifiers used in the BSHR4/PPR is that they should be able to accept a large variation of input power (from different ring nodes) and they should provide near constant output powers (to simplify the receiver design). Compared to a typical seven-node OC-48 (2.4 Gb/s) ring 150 miles long using the conventional implementation (i.e., using a 1 + 1 ADM in each ring node), the BSHR4/PPR may reduce the protection cost by approximately 76 percent [35]. However, the BSHR4/PPR, which uses 1:N protection for electronic components, may be less survivable than the conventional BSHR4 in a scenario involving simultaneous failures of multiple electronic components.

The passive protected self-healing ring architecture can be implemented from a traditional bidirectional four-fiber self-healing ring or upgraded from the bidirectional two-fiber self-healing ring by doubling its capacity with a much lower cost penalty. The capacity constraint of this passive protected ring is limited to the capacity of the working ring; thus, it may still face the same engineering concerns when the capacity is exhausted. To alleviate this growth concern, the concept of "optical ADM" used in BSHR4/PPR can be implemented by using wavelength division multiplexing (WDM) technology. Several examples of WDM self-healing rings have been proposed in [36-39]. These WDM rings potentially could be implemented at high-demand growth areas; however, their cost and performance need to be improved significantly before the technology can be considered a practical approach.

Passive Protected DCS Mesh Networks — According to earlier discussions, the distributed control DCS network may not meet the two-second service objective in metropolitan LATA networks if present DCS network architecture and cross-connect technology remain unchanged. It has also been suggested that the parallel DCS processing, parallel cross-connect architecture and/or ultra-fast cross-connect technology (i.e., less than 10 ms), with a minimum number of restoration messages being processed, may be needed to meet this two-second service objective [25]. Of course, this implies that a significant development effort in upgrading present DCS systems is needed. Also, it is expected that up to 30 percent more cost will be added to the existing DCSs and OLTM due to the spare capacity needed for performing the self-healing function [43]. Combining these two concerns, it would make SONET DCS distributed restoration less attractive for areas that require two-second restoration and cost-effective protection.

The optical network reconfiguration technique may provide a cost-effective alternative in reducing both the network restoration time and network costs. This improvement is due to the use of a passive optical system as a protection system for link and node failures whose system reconfiguration is performed in the all-optical domain and is controlled by electronic network components (e.g., SONET DCS). This passive protected network essentially uses the physical facility protection method, except that it does not duplicate electronic equipment, thus reducing equipment cost. One example of such a passive protected DCS mesh network architecture has been reported in [43]. This proposed passive protected DCS self-healing mesh network architecture is composed of two parts: an electronic working DCS network and a passive protected optical DCS network. The working DCS network may use existing asynchronous DCSs (e.g., DCS-33), near-term SONET DCSs (e.g., SONET B-DCS), or future ATM VPXs for working channel routing in normal conditions and to establish the restoration path when network components fail. The protection optical DCS network transports service signals in case of network failures. The key component in the passive protection DCS network is a special optical cross-connect system (OCS) [43] at each node whose reconfiguration is controlled by the electronic DCS or ATM VPX at the same node. The objectives of this passive protected DCS network architecture are to use an inexpensive OCS to eliminate the need for 20-30 percent higher equipment costs (both OLTM and DCS) for protection, to simplify the restoration operations by using a single restoration path concept, as opposed to the conventional multiple restoration path.
approach, and to use fast optical switching technology to reduce time for protection signal cross-connects. This optical switching may be in few milliseconds for today's electrically controlled mechanical optical switches, which is equivalent to the effect of the next generation switching fabric for the DCS (about 10 ms per STS path [24–25]). This proposed passive protected architecture may work with any SONET DCS or ATM VP self-healing protocol, as described previously. Details of the network architecture and analysis can be found in [43].

Another optical protected DCS self-healing architecture using WDM technology at the ATM VP layer has been proposed in [44]. This new architecture uses a new optical path concept, called virtual wavelength path (VWP). The VWP scheme, which assigns wavelengths on a link-by-link basis, implements a concept similar to VP grouping for fast ATM network restoration [27] but with a much simpler control and provisioning process. This architecture allows the VWP concept to be implemented with commercially available optical technologies, and also allows for consolidating the layered transport architecture and optical technologies.

**Comparison of Layered Protection Schemes**

Table 3 shows a relative and preliminary comparison among different layer protection schemes.

In general, the optical protection layer is still in a very early stage due to its premature technology and lack of network management and operations systems support, although potentially it may restore services very quickly with a reasonable cost, compared with SONET and ATM layer protection. ATM layer protection would require less spare capacity than SONET layer protection at the expense of the slower restoration time and more complex control systems (one exception may be ATM VP self-healing networks versus SONET DCS self-healing networks). How to best use the combination of these three layer protection schemes in the same network remains to be an open issue.

### Standards and Requirements

Table 4 summarizes available standards and Bellcore requirements for survivable network architectures at the SONET and ATM layers. As shown in Table 4, ANSI T1 standards for SONET APS and bidirectional rings have been completed. Requirements for the SONET unidirectional path-switched ring architecture have been defined by Bellcore [10], since it does not require standards efforts. The SONET DCS distributed restoration scheme is still in an early research and development stage, and is not being considered in current ANSI SONET standards. SONET APS systems and self-healing rings of up to OC-48 (both unidirectional and bidirectional rings) have been deployed in LATA networks. For ATM layer protection, APS is currently under discussion in both ITU-T Study Group 13 and ANSI T1S1.5, while the need for ATM self-healing ring protection is under discussion in a working group of T1S1.5. A Bellcore generic requirement document for ATM VP rings using SONET layer protection was released in December 1994 [53]. No standards activity is under way for the VP and/or VC self-healing mesh schemes. No standards and Bellcore requirements exist for passive protected network architectures at the optical layer.

Although there are no standards or Bellcore requirements for passive protected networks, several Bellcore requirements exist for key components of these passive protected network architectures. For example, Bellcore TR-NWT-001073 (issued in January 1994) defines generic requirements for optical switches, and TR-TSY-000901 (issued in August 1989) defines generic requirements for WDM components.

### Layer Interworking on SONET/ATM Networks

To better understand how each layer may interact with each other on SONET-based ATM networks, it would be helpful to explain an integrated network management and control system mode...
<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td>D/C</td>
<td>D/C</td>
<td>D/C</td>
<td></td>
<td></td>
</tr>
<tr>
<td>SONET</td>
<td>APS</td>
<td>T1X.5/95-001</td>
<td>C</td>
<td>COM 15-101-E</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td>(Draft G.SHR-1)</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>SHB</td>
<td>USHR</td>
<td>Study Group (15)</td>
<td>Study Group (15)</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>T1X.5/95-001</td>
<td>C</td>
<td>GR-1400-CORE</td>
<td>3/94</td>
<td>D</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Mesh</td>
<td>No Standards Available</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>ATM</td>
<td>APS</td>
<td>Working Group (T1S1.5)</td>
<td>D</td>
<td>1.0</td>
<td></td>
<td>R&amp;D</td>
</tr>
<tr>
<td></td>
<td>SHR</td>
<td>Working Group (T1S1.5)</td>
<td>D</td>
<td></td>
<td></td>
<td>R&amp;D</td>
</tr>
<tr>
<td></td>
<td>Mesh</td>
<td>No Standards Available</td>
<td></td>
<td></td>
<td></td>
<td>R&amp;D</td>
</tr>
<tr>
<td>Optical</td>
<td>APS</td>
<td>No Standards Available</td>
<td></td>
<td></td>
<td></td>
<td>D/T</td>
</tr>
<tr>
<td></td>
<td>SHR</td>
<td>No Standards Available</td>
<td></td>
<td></td>
<td></td>
<td>R&amp;D</td>
</tr>
<tr>
<td></td>
<td>Mesh</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>R&amp;D</td>
</tr>
</tbody>
</table>

D/C = Draft, C = Complete
(D, T, R&D) = D = Deployed, T = Trial, R&D = Research & Development

Table 4. Standards and Bellcore requirements for survivable network architectures.

As shown in Fig. 8. The model shown in Fig. 8 depicts an interworking scenario among ATM transport, control systems and a network management system. Network control systems here are network protection systems that may be implemented at the SONET layer and the ATM VP layer. The network protection systems at each layer are managed and triggered by the layer management system at each layer, which is then coordinated by the plane management system. The layer management system includes fault management for the "hard" network failures and performance management for "soft" failures (e.g., performance degradation). The fault and performance management systems at each layer are used to trigger either protection switching at the optical layer, SONET layer, or ATM layer, or a re-routing scheme at the network layer that is service and application specific. The function of system (or plane) management is to collect the failure information, interpret the failure messages, identify and isolate the failure location(s), coordinate the timing of generating next higher layer AIS messages, and take necessary actions to recovery failures.

Following is an example that shows the role of system management on network protection across layers. When a cable is cut, the SONET line terminating equipment receives LOS (loss of signal). Here, there are two options: it starts to perform line protection switching (if any), or immediately generates the path AIS and sends it to the downstream path terminating equipment. When the path terminating equipment receives the path AIS, it could initiate SONET path layer restoration (if any), or immediately generate the VP-AIS. Again, when the virtual path terminating equipment (VPT) receives the VP AIS, it could immediately trigger VP layer restoration and does not generate the next higher layer AIS (i.e., VC-AIS) until it completely restores affected signals or a pre-determined time-out period expires. Alternatively, it would immediately generate the VC-AIS and pass it to the equipment-terminating the network layer function (in this case, STP and SCP if the application is for signaling). At the network layer, the system could choose to initiate network re-routing (if any) or just do nothing. At the time this paper was written, there was no standard to guide the timing for generating the next higher level AIS messages from the SONET physical layer to the network layer. However, Bellcore requirements [45] and T1S1.5 agreements in response to a Bellcore contribution have clarified that the VC-AIS is not sent until physical layer protection switching is given a chance to clear the problem. Note that this scenario is based on an assumption that SONET APS and SONET self-healing rings would be universal protection systems for SONET/ATM networks. In reality, SONET APS and SONET self-healing rings may not be applicable to DCS-based mesh networks. Therefore, the waiting period of 50 ms for generating ATM layer alarms would become an unnecessary provision for DCS-based mesh networks that typically carry a majority of demands in the core of LEC networks. In ITU-T, the working group responsible for ATM protection switching agreed in the March 1994 meeting that the ATM layer's AISs should be generated when needed without a waiting period of 50 ms. Thus, an alignment in this timing issue between ITU-T and T1S1 is needed.

If no inter-layer coordination function exists (e.g., no control is applied to control timing for generating the next higher layer AIS messages), the AIS will be passed through each layer after it is generated, triggering the protection switching or self-healing scheme at each layer (optical, SONET, ATM and the network layer) simultaneously. This may create a situation for network resource competition that then causes network congestion or
even network failures. Thus, some inter-layer coordination function is needed to ensure that either the network or ATM layer performance remains acceptable.

Another open issue is how to build a cost-effective survivability scheme across layers (from the optical layer up to the network layer). This involves the identification of unnecessary layer protection that may depend on application requirements, the protection message processing and generating speed, the network size, traffic patterns, and the network budget. For example, in STM transport, transport overhead used to generate SONET layer protection switching is generated and transmitted every 125 μs, while ATM transport allows for many OAM cells being generated and transmitted within a 25-μs time interval as long as the capacity is available. Unlike the STM transport’s OAM fixed capacity, the ATM layer OAM capacity can be assigned dynamically based on needs of the particular maintenance activity or procedure invoked. Thus, ATM transport would be able to convey necessary network protection switching messages faster than its STM counterpart. In [42], it was suggested that ATM VP transport may provide a significant improvement over STM transport for failure detection speed in the range of bit error rate of 10^{-3} to 10^{-5} (e.g., it takes about two seconds and 1 ms to detect BER of 10^{-4} or better for STM transport and ATM VP transport, respectively). This potentially allows for faster network response to “soft” failures by using ATM OAM mechanisms and to “hard” failures by using the SONET line or path AIS mechanism.

**Summary**

We have reviewed possible survivable network architectures and technology for each layer of the SONET/ATM transport network. These layers include the SONET (physical) layer, the ATM layer and a possible optical layer. Tradeoffs and open issues among different survivable architectures for each layer and across different layers have also been discussed. Survivability mechanisms at the ATM layer and a multi-layered system between survivability mechanisms across different layers are still in an early research and development stage. Thus, it is hoped that the information provided here will help stimulate research, development, and standards activities in defining a cost-effective multi-layered survivable SONET/ATM transport network.

**Acknowledgments**

The author would like to thank Haim Kobrinski, Joe Sonnosky and Joe E. Berthold for their valuable comments on the draft, and Carol Adams for preparing some figures for this paper.

**References**

Survivability mechanisms at the ATM layer and a multi-layered system between survivability mechanisms across different layers are still in an early research and development stage.