LIGHTWAVE®

Applications

Innovative component, subsystem, system, and network design examples and alternatives

Fault detection improves network protection

By Richard Jensen

Fiber cuts cause a significant number of disruptions and outages. As businesses and consumers become increasingly intolerant of network failures, downtime can be very expensive to carriers due to both lost revenue and tarnished images. Economic forces have put carriers in the difficult position of simultaneously reducing costs while improving overall network reliability. As a result, carriers continually search for better ways to protect networks against such fiber faults and reduce costs by more efficient use of protection bandwidth.

Integrating fault detection into optical switching at the physical layer can greatly increase the speed of fault detection and protection switching. It can also improve fiber utilization by allowing working lines to share a pool of protection paths. The "shared pool" concept can also enhance network availability by providing protection against multiple fiber faults.

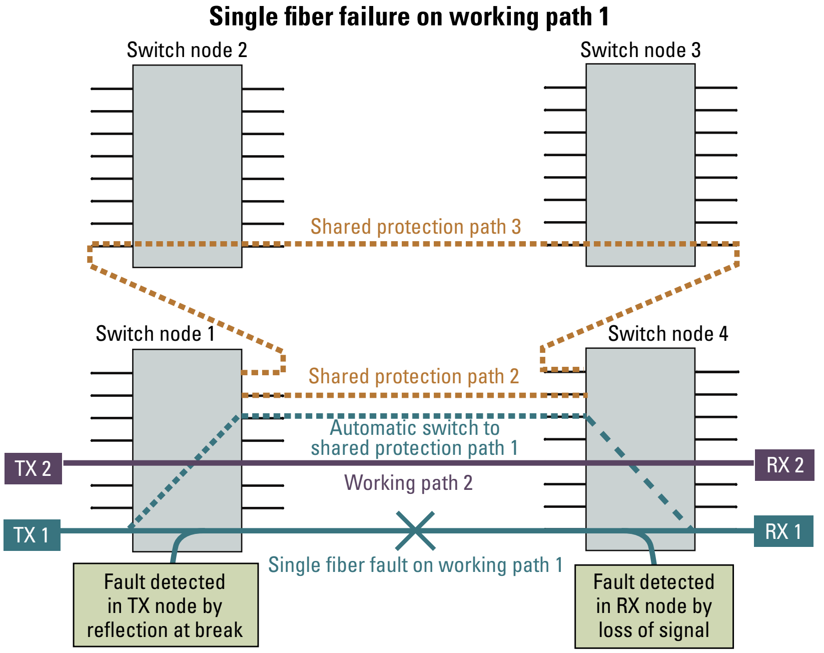
Single fiber failure on working path 1
Switch node 2
Switch node 3
Shared protection path 3
Switch node 1
Switch node 4
Shared protection path 2
Automatic switch to shared protection path 1
Working path 2
TX 2
RX 2
TX 1
RX 1
Single fiber fault on working path 1
Fault detected in TX node by reflection at break
Fault detected in RX node by loss of signal

Figure 1. Optical switches in nodes 1 and 4 detect fiber faults and automatically switch working path 1 to shared protection path 1 without the need for communication between nodes.

Concept and benefits

Integrating fault detection into the optical switch enables faster protection switching because the fault detection and switching can be done locally without the need for overhead signaling among network nodes or higher-level network control planes.

Figure 1 illustrates the concept. When a fiber break occurs on working line 1 it is independently detected by the optical switches at both the transmit and receive ends of the fiber path. After the fault is detected the optical switches automatically perform a protection switch according to predefined rules to protection path 1.

Detecting a fiber break at the receive end can be done by simply monitoring the optical input power. Detecting the break at the transmit end can be done by monitoring for reflections that are characteristic of fiber breaks. Both forms of detection can be accomplished using off-the-shelf optical power detectors.

It is important to note that there are many alternative ways to detect fiber breaks at both the transmit and receive ends of the fiber. The concept of locally detecting faults and automatically switching without the need for signaling is independent of the method used to detect the faults.

This technique is not meant to replace existing protection-switching methods in traditional systems like SONET. In practice it would most likely be integrated into existing systems as an enhancement for handling fiber faults. The optical switch could interface with the higher-level network control planes through a standard communication channel. In the event of a fiber break, the switch would automatically reconfigure around the fault according to predefined rules and then inform the higher-level control plane via the upstream interface. Conversely, the higher-level control planes can command the switch to reconfigure in the event of nonfiber faults or turn off the automatic protection switching feature for maintenance operations.

Two important optical switch characteris-

Reprinted with revisions to format, from the November 2006 edition of **LIGHTWAVE**

tics for this application are very low loss and fast switching times. The low loss minimizes the impact on the transmission line impairment budget; the fast switch time ensures the switching is completed before higher-level control plane layers intervene.

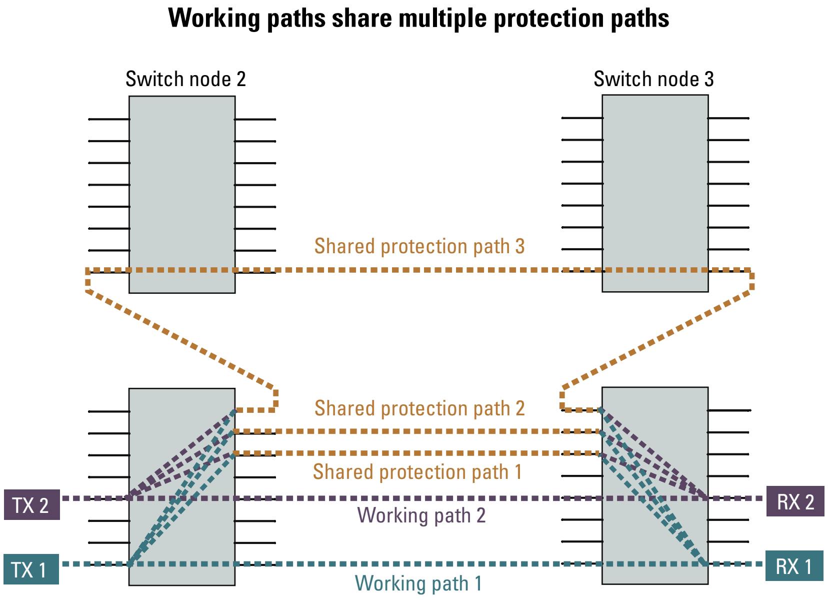

Figure 2. Working paths 1 and 2 efficiently share protection paths 1, 2, and 3. The optical switches automatically select the next available protection path according to predetermined criteria when fiber faults are detected.

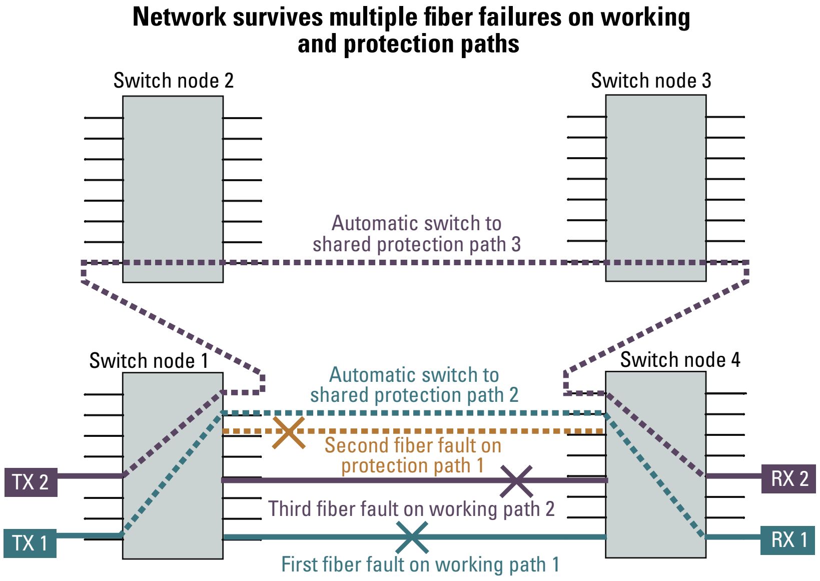
Network survives multiple fiber failures on working and protection paths
Switch node 2
Switch node 3
Automatic switch to shared protection path 3
Switch node 1
Switch node 4
Automatic switch to shared protection path 2
Second fiber fault on protection path 1
TX 2
RX 2
Third fiber fault on working path 2
TX 1
RX 1
First fiber fault on working path 1

Figure 3. Shared protection allows the network to continue operating even with multiple fiber faults. Connection between TX1 and RX1 is maintained even with a fault on working path 1 and protection path 2 by switching to protection path 2. A third fiber fault on working path 2 results in a switch to protection path 3.

The optical switch must also be able to preprovision dark fiber protection paths. Some optical switch technologies need to have light on an input fiber before they can set up a connection, which greatly increases the amount of time required to complete a protection switch and can cause difficulties with bidirectional signals. Switching technologies, such as MEMS, that need light at the input to make a connection cause a cascade of extra switching delay along the line. This effect multiplies the protection switch time by the number of switch connections through which the signal passes. True dark fiber switches do not add any extra delay because the optical path is completely preprovisioned using dark fiber, and only the switching elements at the ends of the optical path need to switch.

The technique described here enables efficient use of protection fiber paths because the local switching control allows the working paths to share a pool of protection paths as shown in Figure 2. The exact protection path for each working path does not need to be defined before a fiber fault occurs. Because the optical switches know which protection paths are in use at any time they simply select the next available protection path and then report the network reconfiguration to the higher network control layers. These higher layers can download updated protection switching criteria at any time.

Shared line protection strategies typically require some sort of communication among the network nodes or some intervention from higher-level network control systems to coordinate the optical switching, and it can be difficult to allow multiple lines to share protection paths. For example, SONET 1+1 and 1:1 are popular protection methods that require communication between two nodes. This variation on shared path protection allows the working traffic lines to efficiently share several protection paths without the need for communication among nodes or intervention from a higher-level network control layer.

The method of how to select the next available protection path can be determined by a variety of means. For example, one simple method would be to preprovision dark fiber protection paths and predetermine the order in which they will be assigned to mitigate faults. This scheme enables multiple working paths connected to the switch to efficiently share a common pool of protection fibers and paths.

Designing networks that are automatically protected against multiple worst-case fiber breaks can be difficult and expensive. As a result, many network protection schemes typically only provide automatic protection against single fiber faults. The reasoning behind this is that a repair crew will be dispatched immediately after a single fault and hopefully fix the problem before another fault occurs.

Major disasters, like earthquakes and hurricanes, can often cause multiple fiber breaks in a network. The “shared pool” concept can be extended to the difficult task of protecting a network against multiple fiber breaks by simply monitoring the protection paths in the same way as the working paths after they are provisioned. This allows the traffic-carrying protection paths to be protected by the remaining resources of the shared pool. If the network experiences a second fiber break on either a provisioned protection path or regular working line, the traffic is automatically switched to another protection path from the pool as shown in Figure 3.

The number of faults the network can tolerate is determined by the size of the spare fiber pool. While no system can protect against every contingency, having a network that can automatically reconfigure and recover from multiple fiber faults will greatly improve overall availability.

Testing the concept

To test this concept we assembled a network of four Polatis matrix optical switches equipped with fault detections (two 16×16 switches and two 8×8 switches). The maximum loss of any optical switch connection, including the fault detectors, was 1 dB. The switches were interconnected with lengths of fibers. The protection paths and their order of use were programmed into the switch hardware. Four laser sources and detector pairs were used to simulate traffic. An Agilent OC-192 SONET test set was used as a fifth traffic source to measure fault detection and switch times.

Fiber faults were simulated by disconnecting fibers. The results showed that faults could be detected and the protection switch completed in less than 10 msec. This interval is about six times faster than the current SONET performance benchmark, which allows for 10 msec to detect a fault and then 50 msec to complete a protection switch. Follow-on work to further optimize the technology looks promising to reduce the fault detection and switch time to under 5 msec, which would be more than 10 times faster than the SONET benchmark. The shared pool technique was used to demonstrate network survivability with four fiber worst-case faults on the same transmit/receive pair.

Integrating fiber fault detection into optical switching opens up options to enhance network protection and availability. The combined technique can decrease the protection switching time and allow efficient use of shared protection resources. The shared protection pool concept can be integrated with traditional network protection systems and extended to cover multiple fiber breaks. Concepts like these can help alleviate the pressures on service providers by lowering costs, enabling the more efficient use of existing resources, and improving the network availability.

Richard Jensen *is director of network architecture at Polatis Inc. (www.polatis.com).*