

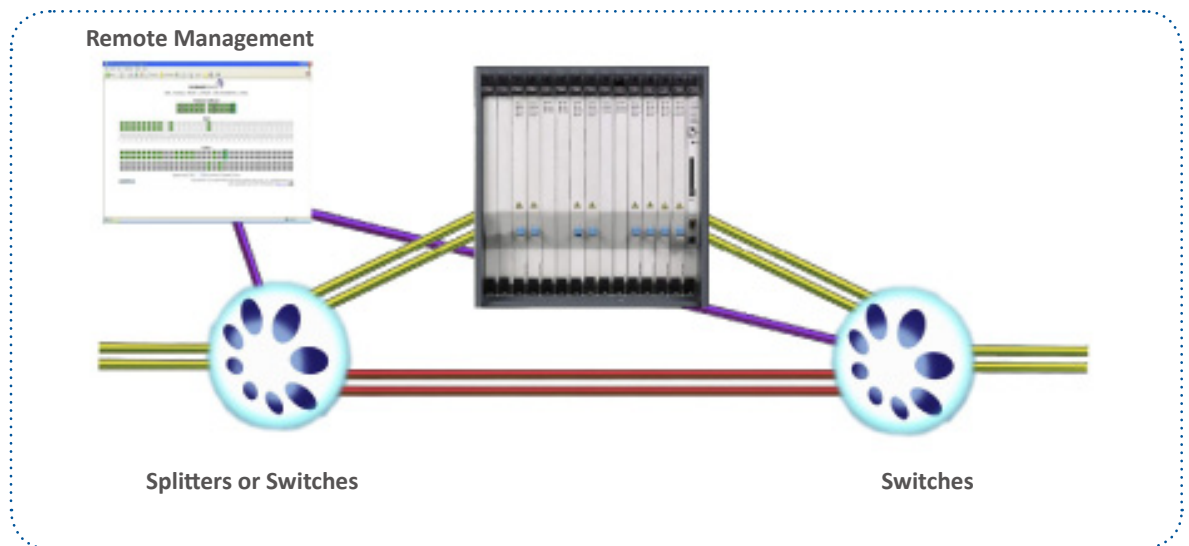
The Gold Standard for availability in the Telecommunications Industry has always been the five 9's requirement, or 99.999% up time. This translates to only a few minutes of down time per year. In today's network, this standard is becoming increasingly difficult to meet or verify. Most of the equipment outages today are software related. With the rapid migration to IP, the software content of telecommunications equipment will only increase, with the accompanying increase in outages.

Furthermore, with the ever increasing line rates, the impact of an outage, no matter how short, is becoming more severe. This is leading to the increased usage of photonic switching to minimize the cost of outages by rapidly recovering from equipment failures. This Application Note describes three different levels of equipment protection utilizing photonic switching.

**Photonic Bypass Switching**

The simplest and least expensive method of recovering from an equipment failure is to route traffic around the failed unit. While simple, this method is not always feasible. For example, it is not possible to simply bypass a failed DWDM transponder. However, if the alternative is to drop all traffic, it may be preferable to quickly bypass the failed unit. For example, if a deep packet inspection unit fails, it preferable to lose the inspection functionality rather than to lose the traffic.

Bypass can be implemented at the photonic layer by using either optical splitters or 1x2 switches in front of the unit to be bypassed and 2x1 switches afterwards. In this way, traffic is normally switched through the unit and upon a failure redirected to the bypass fiber(s). The decision to use optical splitters vs 1x2 switches is made by weighing the higher optical loss of the splitters with the increased complexity of managing the 1x2 switches.



**Figure 1. Photo Bypass**

**Create**

**Monitor**

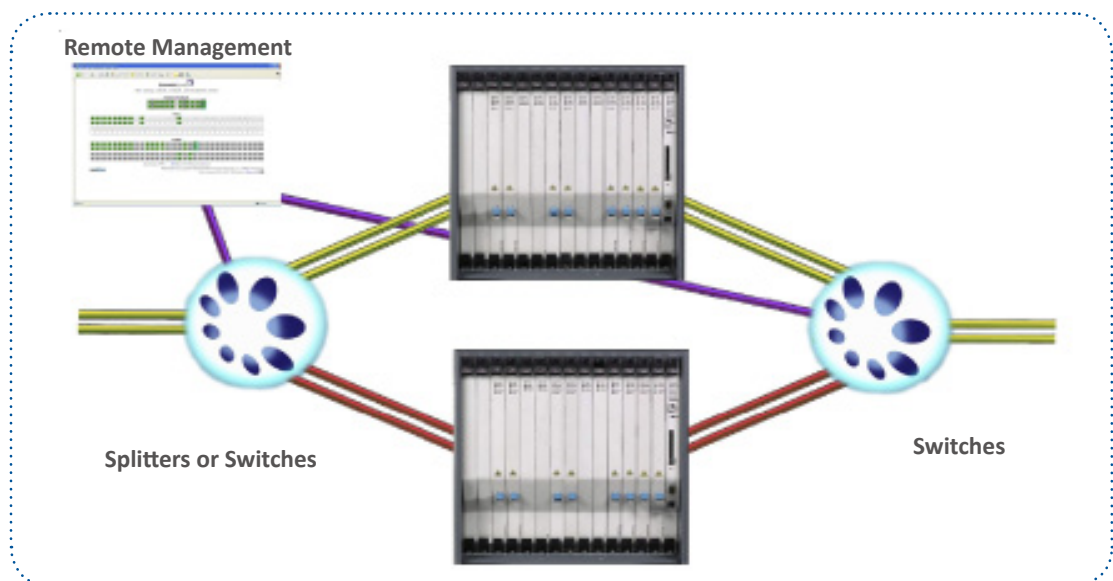
**Reconfigure**

Note that if there are a large number of fibers providing traffic to/from the unit then it may be more desirable to implement Photonic Bypass using full photonic crossconnects instead of legions of splitters and small switches. In addition to easier management, there are added operational benefits to photonic crossconnects which will be discussed below.

### 1:1 Protection

If Photonic Bypass is not practicable, or desirable, then full equipment redundancy can be implemented. Analogous to traditional SONET protection, this requires a hot spare unit for each working unit. In the event of the failure of the working unit, traffic is switched to the hot spare. Note that in addition to switching the traffic to the hot spare, OSS level tasks may need to be performed to configure the hot spare to handle the traffic.

1:1 Protection can be implemented at the photonic layer exactly the same way that it is in Photonic Bypass. The only difference is that the Bypass path now includes the hot spare unit.



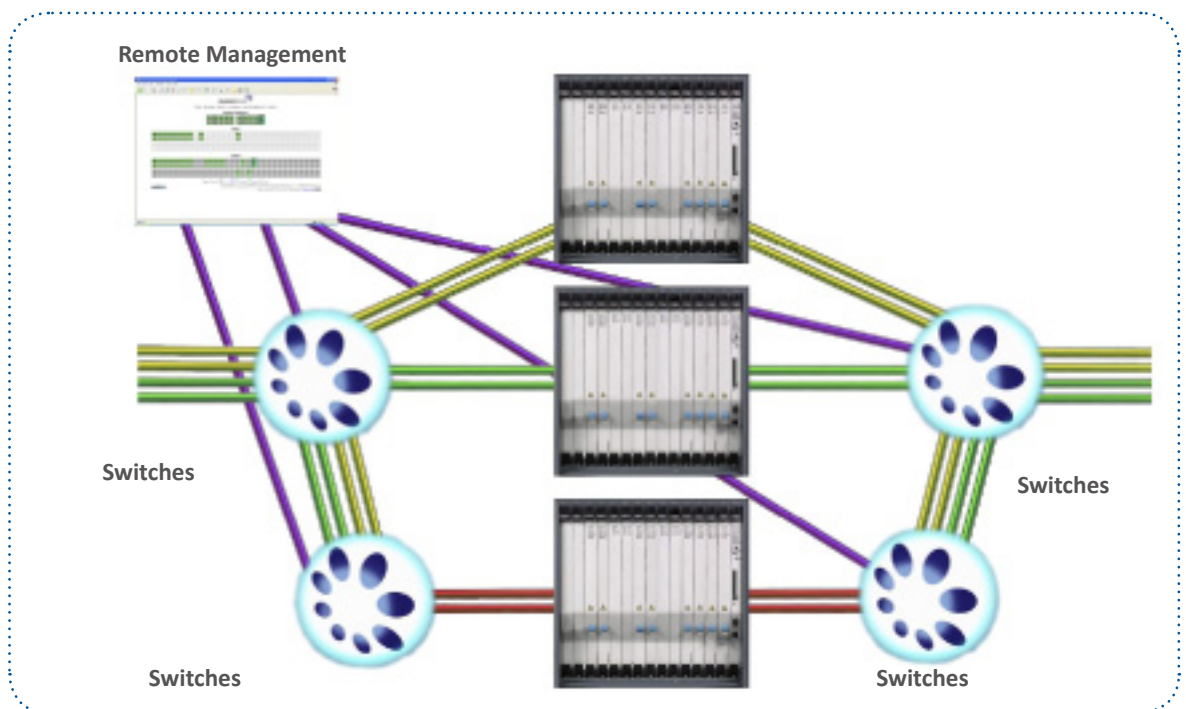
**Figure 2. 1:1 Protection**

### N:M Protection

A major complaint about 1:1 Protection is the cost of maintaining a hot spare for each working unit. N:M Protection reduces the equipment costs by sharing the hot spare among several working units. For example, a single hot spare could be used to back up 4 working units. Or, if multiple failures are a concern, a small pool of hot spares would be used back up a larger pool of working units. Note that, as in the case of 1:1 Protection, in addition to switching the traffic to the hot spare, OSS level tasks may need to be performed to configure the hot spare to handle the traffic.

Implementing N:M Protection is more difficult than Bypass or 1:1 Protection since each hot spare must be able to receive traffic meant for any of the N working units. Likewise, traffic from each hot spare must be able to replace traffic from any failed working unit. Two implementation schemes are possible.

First, traffic to each working unit is split between the working unit and the M protection units. This could be done with either 1:(M+1) optical splitters or 1x(M+1) optical switches. An additional Nx1 switch would be required to select the traffic destined for each protection unit. Similarly (M+1)x1 switches would be required for each output to select between the working unit and the M protection units, with an additional 1xN switch on the output of each protection unit.



**Figure 3. N:M Protection With Splitters and 1x Switches**

However, large splitters have high loss. A second approach uses full crossconnects. As shown in Figure 4 below, a single Nx(N+M) crossconnect is used to direct the N incoming traffic paths to the working and protection units and, correspondingly a single (N+M)xN crossconnect would be used to select the sources for the N outgoing traffic paths.

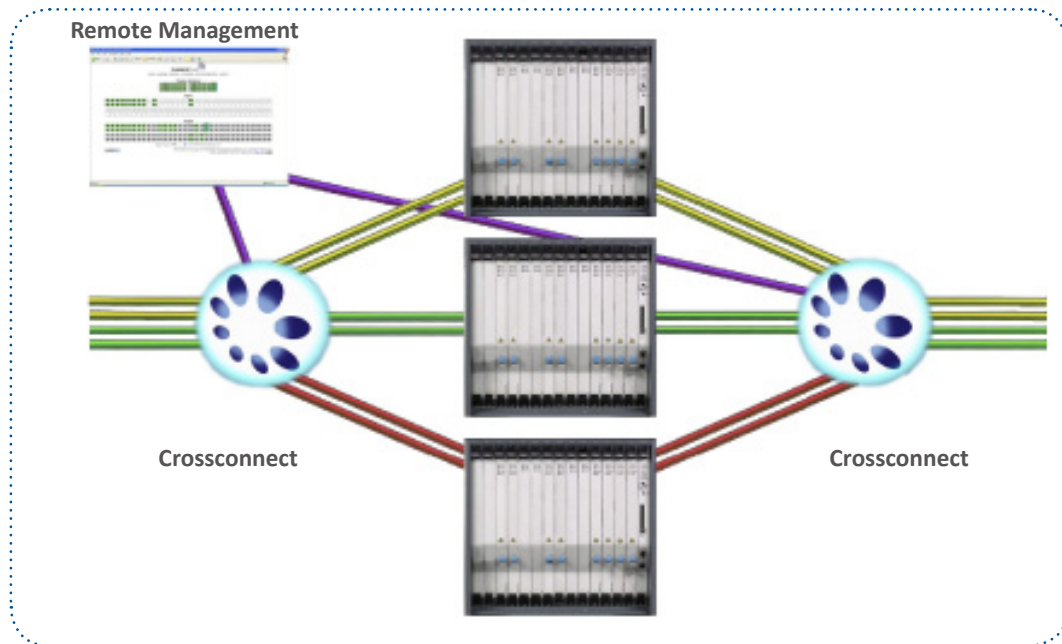


Figure 4. Crossconnect-based N:M Protection

### Fault Detection

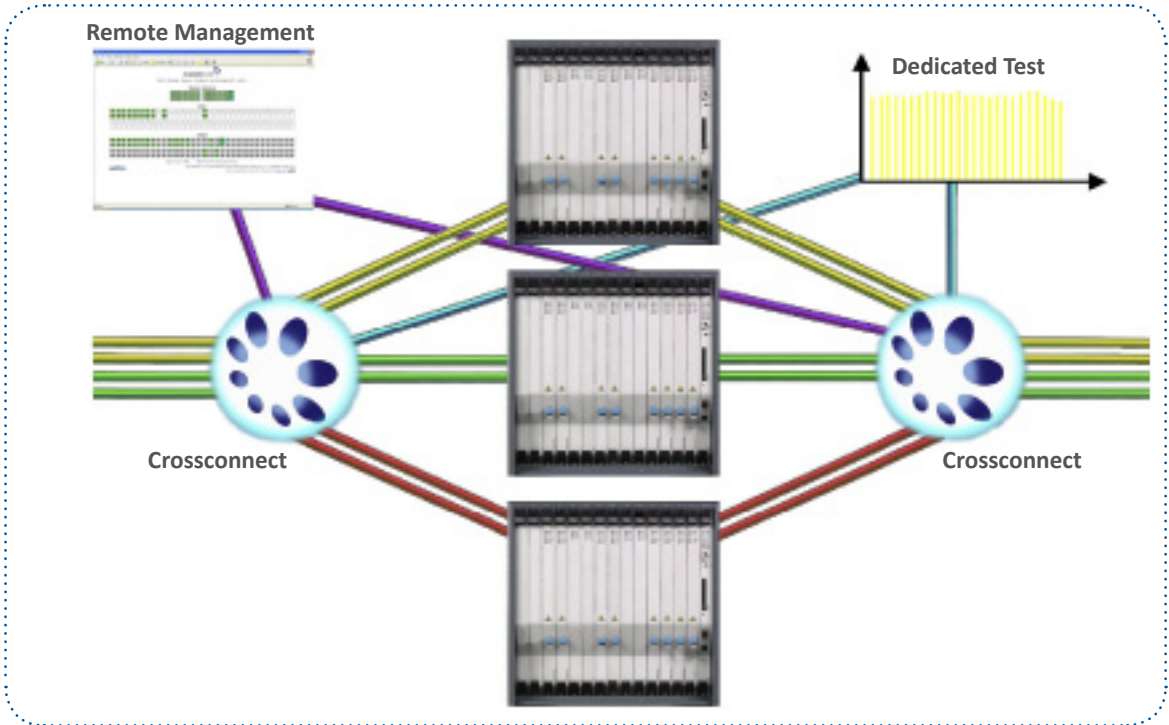
Another facet of Equipment Protection which has become more complex in today's networks is the determination of when a protection switch needs to occur. As opposed to fiber protection, it is not sufficient to switch only on loss of light thresholds. Equipment failures do not necessarily result in the failed equipment turning off its lasers. Thus, in addition to loss of light, it is necessary for the equipment protection system to react to alarms and fault traps from the failed equipment and to react to response failures from active "pinging" of the equipment (i.e. a deadman timer). Alternatively, an upper level OSS may detect the failure and direct the photonic switches to switch.

### Added Benefits of Photonic Crossconnects

While Equipment Protection can be implemented with passive optical splitters and small 1x2 and 2x1 switches, there are additional benefits, above and beyond protection, to an implementation with full photonic crossconnects.

First, non-blocking crossconnects have the flexibility required to chose different levels of protection for different traffic streams and to rapidly and remotely change those assignments as requirements change. For example, the network operator could direct that certain light paths bypass the unit if it fails, while other, higher priority, light paths would be directed to a smaller hot spare.

Second, having a full crossconnect facilitates pre-failure monitoring and post-failure problem diagnosis. Once the protection switch has occurred, loopback paths can be implemented quickly through the crossconnect to help isolate problems. In addition, extra ports on the crossconnect can be dedicated to test equipment which can be switched in as needed to monitor traffic and/or to assist in the diagnosis of a failed unit.



**Figure 5. Enhanced Test**

### Summary

Network equipment is becoming increasingly complex and increasingly software intensive. The use of photonic switches, ranging from simple 1x2s to large crossconnects, provides the flexibility required to rapidly recover from equipment failure at a cost which is far below any electronic switching alternative.

Glimmerglass Optical Cyber Solutions  
26142 Eden Landing Road  
Hayward, CA 94545 USA

Headquarters  
Phone: 877.723.1900  
In North America: 510.723.1900

Americas and Federal Sales  
Phone +1 510 723 1925  
Fax +1 510 780 9851

Middle East and Africa  
Sales  
Phone +1 510 461 2990  
Fax +1 510 780 9851

Asia-Pacific Sales  
Phone +852 2857 6308  
Fax +852 2857 6260

Europe Sales  
Phone +44 1590 636583  
Fax +44 1590 681308

sales@glimmerglass.com

**Glimmerglass**   
Optical Cyber Solutions