

# Fault Isolation in the Agile Transparent Network

K. Johnson, B. Yuan

*Innovance Networks, 19 Fairmont Avenue, Ottawa, ON, K1Y 1X4, CANADA*

*Tel. +613 798 9293, Fax. +613 798 0954, email: kjohnson@innovance.com, byuan@innovance.com*

## Abstract

The drive to reduce backbone network cost has been the catalyst for many advances in optical networking technologies. Over the past 5-7 years, improvements in system reach through enhanced modulation schemes and optical amplification have led to ultra long haul systems capable of transporting DWDM wavelengths 1000's of kilometers. Recent advances in photonic switching have enabled transparent networking of DWDM wavelengths. Migrating to a transparent network architecture that supports end-to-end wavelength networking and removing unnecessary optical-electrical-optical (OEO) conversions at pass-through switching nodes results in network cost savings as significant as 40-50% [1]. Adding full spectrum tunable sources and filters provides significant operational savings and offers a new level of flexibility and DWDM provisioning speed. These capital and operational savings and speed of connection activation are key attributes of next generation agile networks.

The capital savings alone provide a compelling reason to minimize OEO conversions in the network. However, one of the drawbacks commonly attributed to transparent networking is that removing OEO points from the network limits fault isolation capabilities. Although this can be true in a completely transparent network (all optical with no OEO conversions), the backbone network realities dictate the need for some OEO conversions. The need for grooming, wavelength conversion and regeneration still require some amount of OEO conversions in the backbone network. In this paper, an agile transparent network is considered, where the use of OEO conversions is optimized. This paper describes how tunable technology, transparent switching, enhanced optical monitoring and system intelligence associated with an agile transparent network can provide better fault isolation than traditional point-to-point DWDM implementations.

## Introduction

Opaque networks constructed with point-to-point DWDM line systems provide the ability to monitor wavelengths at all interconnect points since each wavelength is electrically terminated. This approach, however, introduces unnecessary cost into the network since the majority of wavelengths are merely reconnected to another line system through back-to-back opto-electronic converters. Transparent networks eliminate most of these back-to-back conversions, thus electronic monitoring points (and their associated costs) are typically only located at network ingress and egress points. In both opaque and transparent networks, the key goal remains the same: detection of degradation as soon as it occurs and isolation of the fault to its root cause.

In order to provide timely resolution to performance degradations, carriers require methods to quickly isolate faults to a single fiber span or replaceable module. The question is what tools can be used in a transparent network to provide the required fault isolation, and how do these tools compare to the existing ones? There are two keys to answering this question. The first is to understand, in general, the types of faults that can arise in a network. The second is to understand existing troubleshooting methods and how "new" methods and tools can be applied in transparent networks.

## **Fault Classification**

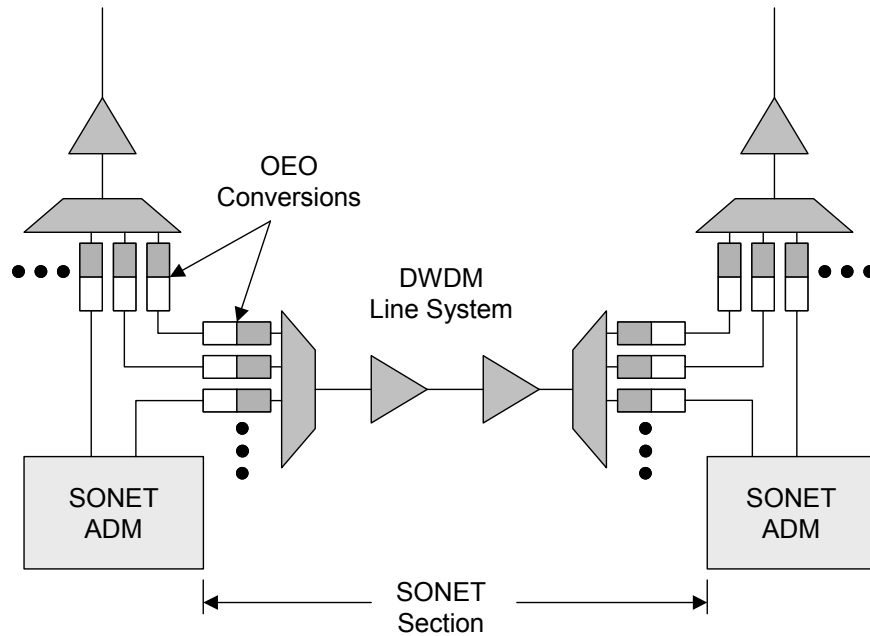
This paper classifies faults into two broad categories: hard faults and soft faults. Hard faults encompass failures in the physical equipment or medium used to provide the service. These failures are not transitory in nature, and they require that equipment be repaired or replaced before the service can be restored. In addition, hard faults are typically detected immediately, and at least one alarm is generated. Circuit pack failures and fiber cuts are common examples of hard faults. A hardware fault point normally detects a circuit pack failure immediately, while a fiber cut is detected when the downstream node sees the loss of light and alarms the resulting condition.

Soft faults, on the other hand, are performance degradations to a service where an associated hard failure cannot be attributed. Soft faults either temporarily interrupt or simply degrade the performance of the service. The main difference between soft and hard faults is that soft faults are detected downstream (sometimes several fiber spans downstream) from where the fault originates, preventing the immediate identification of the root cause of the failure. Advanced fault correlation software is required to determine the root cause. Stretched or kinked fibers; degradations due to aging; and environmental factors are all examples of soft faults. Tools and techniques for troubleshooting and identifying these faults are discussed later in this paper.

## **Traditional Diagnostic Approaches**

In core networks, SONET fault isolation techniques are used in conjunction with DWDM optical monitoring. This section briefly describes the traditional SONET approaches for isolating degradations with performance monitoring and maintenance signaling for hard fault isolation.

The general strategy for detection and isolation of soft faults in today's network is to use SONET performance monitoring. With point-to-point DWDM systems, BER and related data such as SONET PMs are available at line system interconnect points. As shown in Figure 1, this is possible because back-to-back OEO conversions are performed on each wavelength. In the simplified example shown in Figure 1, there are no intermediate SONET regenerators so the SONET section and line extend between the SONET ADMs. SONET section statistics, computed using the B1 byte in the section overhead, are used at handoff between SONET equipment and the DWDM line system. Each wavelength can be monitored at its endpoint to determine its health.



**Figure 1 – Traditional Fault Sectionalization based on SONET Performance Monitoring**

In cases where a DWDM transport system is used to transport the signal between regeneration points, further fault segmentation will be required using analog measurement tools. At amplification sites, the multi-wavelength signal is analyzed using analog measurements such as total received optical power. Often, this is accomplished by comparing current power readings to a historic baseline value recorded when the system was first commissioned. Reflection measurements are also commonly used in the process of isolating a fault within a DWDM line system.

To assist in hard fault isolation, SONET supports Alarm Indication Signal (AIS) and Remote Defect Indication (RDI) maintenance signals to provide upstream awareness of faults and downstream fault indication conditioning. For example, if a fiber cut occurs, it will be immediately detected by the downstream node, which will assert a loss of signal (LOS) alarm indication. In order to squelch symptomatic alarms downstream, the network element detecting the LOS condition will assert an AIS signal in the line overhead. The downstream LTE will terminate the incoming line AIS signal and generate the appropriate path level AIS signals. In the case of a unidirectional failure, a RDI message is sent to the upstream nodes to notify them of the failure and to initiate channel conditioning. Generally, the RDI signal is used to facilitate restoration activities in the upstream equipment. From a fault isolation perspective, RDI and AIS indications provide an indication of the SONET section where the fault occurred.

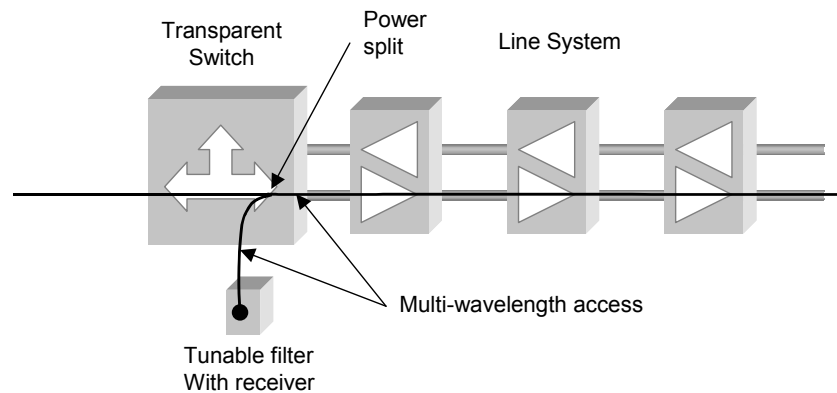
These SONET mechanisms provide a method to isolate hard faults to a specific section within a SONET line. However, additional fault isolation of the DWDM layer is required. This is often based on optical loss of power indications at line amplifier sites. Often in DWDM line systems, the symptomatic downstream alarms are not suppressed and require correlation software or human analysis.

## Agile Transparent Networking Introduces New Capabilities

To support dynamically configurable (agile) transparent networking, a number of new capabilities have been introduced into the DWDM layer. A significant byproduct of these capabilities is improved fault isolation. These capabilities include:

- Transparent switching for interconnect between line systems
- Tunable sources and filters to permit wavelength assignment at provisioning time
- A distributed control plane that understands network topology and considers photonic properties and constraints for wavelength routing
- Advanced control software to provide end-to-end wavelength monitoring and control
- G.709 Digital Wrapper

Hierarchical transparent switching - where interconnection between the line system and switching node is performed at the multiplex level - provides a single point where all incoming wavelengths can be monitored. A simple power tap on the multiplexed line at the switch input port provides access to all wavelengths on the line. Since the test access port is a power split, this monitoring can be done in a non-intrusive fashion. This multi-wavelength signal can be connected through a tunable filter to a receiver to select a specific wavelength of interest. From this point, the signal can be monitored in the digital domain, which provides the same diagnostic capabilities as a OEO conversion point between line systems in a point-to-point DWDM network. In this paper, this technique is referred to as “optical eavesdropping”.



**Figure 2 - Transparent switch and tunable filter enable digital monitoring**

Another important characteristic of an agile transparent network is a distributed control plane that performs dynamic wavelength routing and activation. To compute the lowest cost end-to-end connection the control plane must be aware of network topology and photonic properties of the fiber plant and optical components. For example, to assign an appropriate wavelength, the fiber losses and dispersion characteristics for each span must be known and used during wavelength assignment. Also, detailed knowledge of the optical components associated with the connection, such as noise figure, chirp and dispersion are factored into the photonic engineering logic of the control plane. As a result, automated engineering can adapt to the actual performance of installed components and guarantee performance over the life of all associated wavelength connections. Embedded measurement capability and embedded performance data in each component can be used to provide an expected performance for each connection. Significant deviations from this expected value indicate the potential for soft faults. An audit that follows the optical path can

quickly compare all of these performance criteria against measured values to show points in the network at which components are operating in the margins, a potential cause of soft failures.

Transparent wavelength networking also introduces a number of challenges for DWDM control system software. To effectively support arbitrary length optical paths introduced by differing wavelength ingress and egress points, intelligent optical control loops are needed in both the line system and transparent switch. Line control loops manage gain profiles as wavelengths are added or removed from the line segment. These control loops are needed to control Raman gain, EDFA tilt and dynamic gain equalization. Advanced line control methods require strategic monitoring taps and per channel feedback through an Optical Spectrum Analyzer (OSA). At wavelength endpoints and switching points, control loops are required to control per-wavelength power launched into the line and delivered to the transceivers. Again these control techniques require monitoring taps and per channel feedback through an OSA.

Adding and removing wavelengths from a transparent network requires network level coordination between the control domains to ensure end-to-end performance. To perform its function, the network level intelligence must understand the network topology. This higher-level control function falls into the realm of a distributed control plane. The key functions in the control plane that enable network wide wavelength control are collection and distribution of topology and photonic layer parameters throughout the network. The information collected by the wavelength control system provides insight into wavelength performance at several points throughout the network.

Finally, to contend with the long transmission paths necessary for transparent networking aggressive forward error correction (FEC) is used. To provide FEC, incoming signals are framed in an ITU G.709 [2] based digital wrapper. This wrapper contains many features, described below, that are relevant to fault segmentation and isolation. These features can be accessed wherever an OEO conversion is performed in the network.

The FEC overhead and BIP-8 parity bytes facilitate signal monitoring with measurements similar to SONET, such as code violations, errored seconds and severely errored seconds. These measurements provide a detailed indication of signal quality. When this is combined with the “optical eavesdropping” technique described above, performance degradations can be isolated to a single multiplex section between optical switching sites.

Another special feature of the digital wrapper overhead is the support for tandem connection monitoring. This permits the operator to define the section to be monitored instead of being restricted by the SONET section/line/path hierarchy.

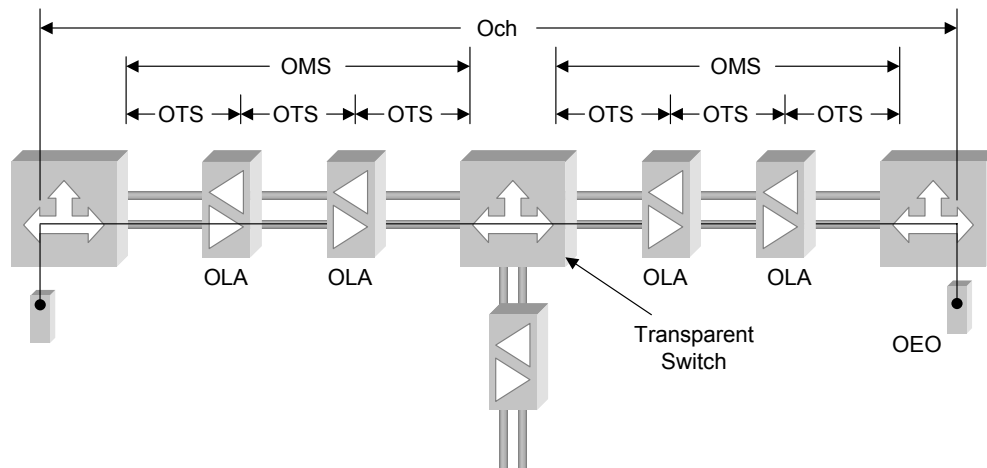
Digital wrapper trail trace monitoring performs a function similar to that provided by the path trace byte in the SONET overhead. The trail trace overhead can be correlated with expected values to ensure that the signal is following the expected path.

## **Soft Fault Isolation**

As described earlier, isolating a soft fault in a traditional DWDM line system can be a complicated and time-consuming task, since it requires the user to compare the current power measurements to historical baseline values. Using this technology to troubleshoot a fault in a long haul transparent system could be difficult, since path lengths can span thousands of

kilometers without electrical monitoring points. Fortunately, a new generation of tools, which will be described in this section, have been developed to facilitate this process.

In order to understand how these tools are used, it is important to explain some terminology that is used in the transparent network. As defined in ITU G.872 [3], optical networks contain several layers just like SONET networks. At the “path” level, optical networks support Optical Channels (Och) which track the service end-to-end from where it enters the transparent network as a digital signal to where it exits. Similar to the “line” concept in SONET, the Och layer is composed of many optical multiplex section trails (OMS). Optical multiplex sections (OMS) are delimited by locations where the signal is multiplexed or switched into other line systems. The OMS layer is composed of several OTS trails. These represent the physical medium that is used to transport the optical signal between network elements in the OMS. The relationship between all three layers is illustrated in Figure 3.



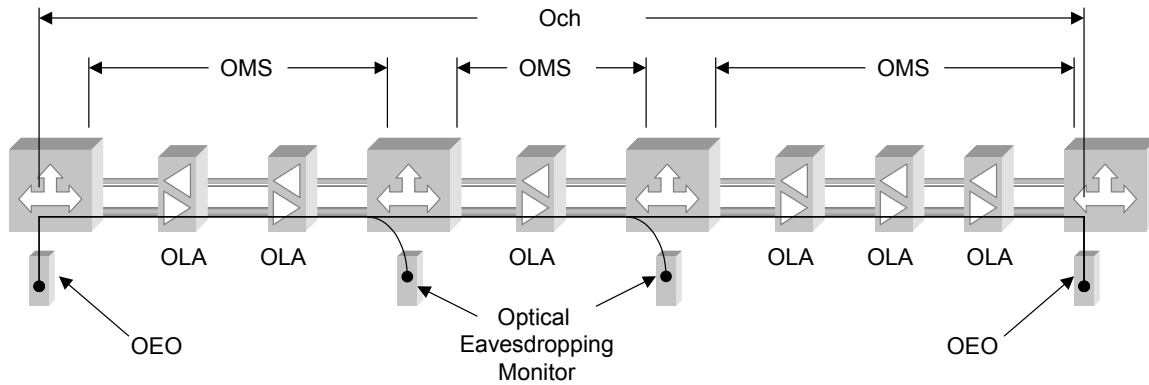
**Figure 3 – OTN Layers in for a sample Och Trail**

In a transparent system a soft fault will be indicated by a threshold crossing alert on the Och trail at the OEO point where the signal exits the network. From this, all portions of the Och trail are suspect. The first step in isolating the fault is to segment the fault to an individual OMS trail. The next step is to isolate the OTS trail within the OMS trail that contains the fault using optical power and reflection readings. This can be accomplished using traditional tools, but a new generation of tools will dramatically reduce the amount of time required by this process. The steps and tools that can be used to isolate a fault will be described in greater detail in the following section.

## OMS Fault Isolation

The first step in isolating a soft fault within a transparent network is to determine which OMS trail is causing the fault. Typically, OMS trails originate and terminate on flexibility (switching) sites such as optical switch network elements and OADM's. One mechanism to isolate faults to an individual OMS trail is to force regeneration at a flexibility point. When signal regeneration occurs, an OEO conversion takes place, which permits the estimation of the signal quality using a BER measurement. This mechanism has two drawbacks. First, forcing regeneration disrupts the existing signal path. Second, adding regeneration into a signal path increases the overall cost of the circuit as described in the abstract.

The preferred mechanism for segmenting Och faults to an OMS trail is eavesdropping. Eavesdropping uses spare tunable filters and receivers (or dedicated test tunable filters and receivers) at network flexibility sites. A small amount of power is tapped from the bearer signal of interest to an unused receiver. An OEO conversion is performed at the receiver to estimate the BER of the originating bearer channel. The advantage of this technique over forced regeneration is that the signal monitoring is non-intrusive to the existing service.



**Figure 4 - OMS Fault sectionalization based on eavesdropping**

## OTS Fault Isolation

Once the fault has been isolated to a specific OMS trail, analog tools must be used to further isolate the fault down to a single replaceable module or fiber. As described previously, manual comparison of the current power readings to “baseline” power readings was the traditional method for fault isolation. While effective, this could be quite a lengthy and time-consuming task. The key to rapid detection and isolation to an OTS trail is the rapid measurement and correlation of relevant power measurements.

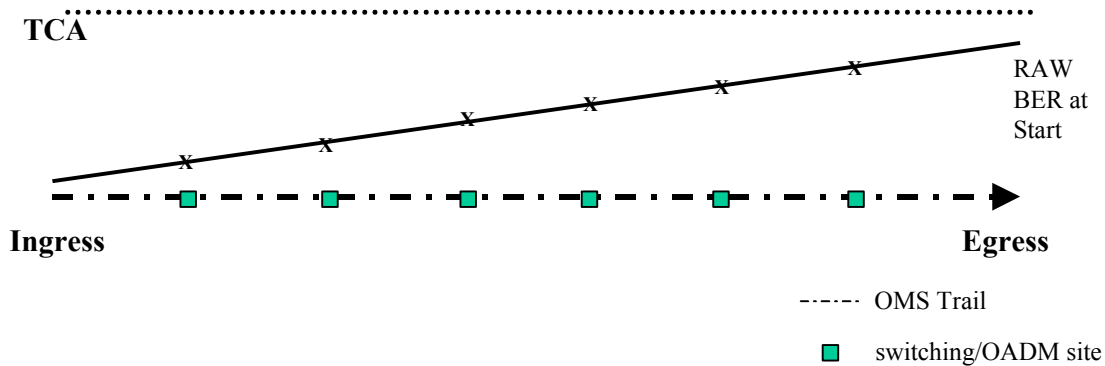
The first step in isolating faults to an OTS is to gather all of the analog power measurements that are relevant to the trail of interest. There can be hundreds of potential monitoring points in an OMS trail. Data of interest include total and reflected power measurements as well as individual channel measurements.

Once all of the relevant monitoring points have been located, the next step is to automatically compare them to their expected value. While this could be a simple comparison to a baseline value as seen in earlier systems, advanced fault isolation systems will pre-calculate the expected loss between monitoring points based on the components, connectors, and fibers used. The pre-calculation of the expected loss enables automatic identification of potential problem spots within the OMS trail. Here, the measured loss will be much higher than the expected loss in fault scenarios. Problem spots can then be brought to the users’ attention.

Ideally, these features are packaged into an advanced fault correlation software tool for troubleshooting problems in a transparent network. This software tool would follow the trail in question, reading all relevant analog and digital performance measurements on the selected channel and compare them to the expected values to detect unusual system events. Unusual readings are automatically flagged for the operator’s attention.

## Soft Fault Isolation Example

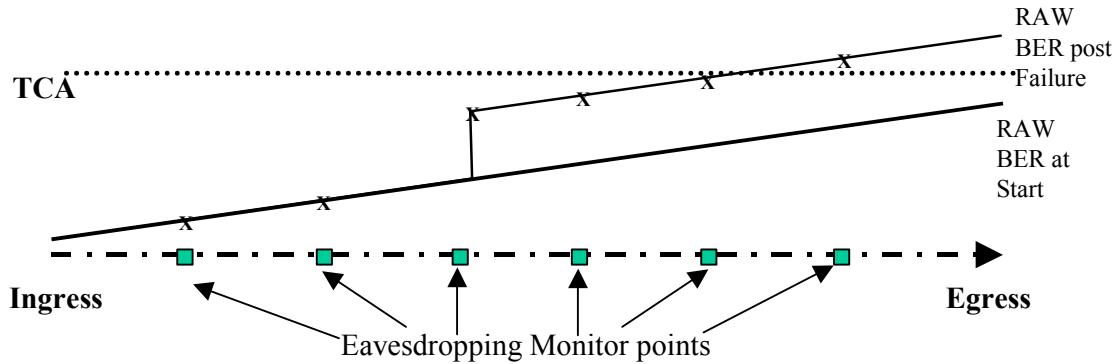
In certain operating scenarios, a dirty fiber and some specific component failures will be difficult to detect as a hard failure. Instead, these degradations will become visible when the signal is converted back into an electrical format. BER will rise and cross a preset threshold, asserting a Threshold Crossing Alert (TCA). This scenario is the perfect candidate for the soft fault isolation tool previously described.



**Figure 4 – BER Curve for OCh Trail without impairments**

The digital wrapper PM data performs a critical role in detecting the soft fault by providing the BER measurements that are compared to thresholds. Under normal operating conditions, the fault correlation software will periodically measure the BER of a trail at all monitoring points in the network. As shown in Figure 4, the fault monitoring software measures the signal BER at eight different monitoring points along the signal path (two endpoints and six intermediate points). Each monitoring point represents a switching or OADM site, with OMS trails interconnecting the sites in the network. In the normal operating conditions illustrated in Figure 4, the BER for the signal remains below the threshold that triggers a TCA event. The fault correlation software periodically captures all of these readings for future reference.

In the component failure scenario, the failure causes a degradation of the signal, thus causing BER to rise at egress, and a TCA to be raised. As shown in Figure 5, the degradation occurs between the second and third monitoring points, thus dramatically increasing the overall BER of the signal. The ability to “eavesdrop” provides the vital data required to isolate the fault. Advanced fault correlation software automatically eavesdrops on the signal at all eight potential monitoring points in the path. This provides a BER measurement for each OMS trail. This measurement is compared to historical values to determine the OMS trails of interest.



**Figure 5 – BER Curve for Och Trail with component failure impairment**

In this example, the fault isolation software notes a sudden increase in the BER between the second and third monitoring points.

Advanced fault isolation and correlation software is executed on the noted OMS trail to gather relevant analog power and reflection readings. These values are compared to expected values, and any losses outside the expected ranges are reported to the user for further analysis.

## Hard Fault Isolation Techniques

Hard faults in the transmission path are readily detected since there is a loss of continuity, which can easily be detected at the Och endpoints. In a transparent network a fiber span will contain wavelengths that ingress and egress the network at different nodes, causing several network elements to detect the loss of signal condition. To avoid superfluous alarm reports at connection termination points the fault management system provides fault indications to downstream nodes in a manner similar to SONET. This is accomplished by sending Forward Defect Indications (FDI) over the optical supervisory channel (OSC), as defined in ITU G.872. In addition, the fault management system requires knowledge of the network topology and relationship between OMS and Och layers to condition downstream alarms.

For example, as shown in Figure 6, alarm indications in the event of a fiber cut can be conditioned so that the root cause can be quickly detected. In the event of a fiber cut, the line amplifiers adjacent to the cut send FDI messages over the OSC to the nearest downstream nodes indicating a failure. Using the network topology, the switching nodes determine the end points of all affected connections and, in-turn, send FDI messages to the endpoint network elements. When the FDI indication is received, the channel loss of signal can be conditioned (converted) to a lower severity alarm at the endpoints. This provides a clear alarm indication of the root cause at the amplifier sites and an indication of affected channels at the endpoints.

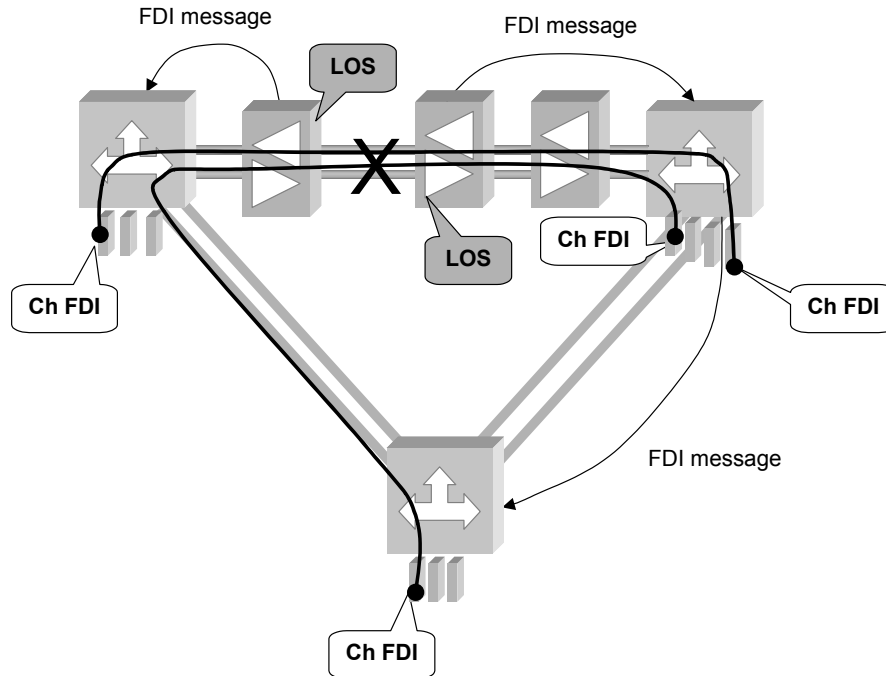


Figure 6 - Alarm conditioning with G.872 messaging

## Conclusion

Faults isolation in an agile transparent network can be made simple for the network operator. ITU-T Recommendations define network layering and maintenance messaging that provides hard fault isolation capabilities equivalent to those found in SONET. Techniques and tools for isolating soft faults in an agile transparent network improve upon existing point-to-point DWDM implementations. Optical eavesdropping provides an equivalent to monitoring at OEO conversion points. The improvements come from a distributed control plane with network topology awareness, increased photonic monitoring, embedded optical component performance information and intelligent fault isolation tools that automate data collection and analysis.

## References

- [1] J. Frodsham, A. Solheim, "Next-Generation Backbone Network Metrics", in NFOEC 2001 Technical Proceedings, Baltimore, August 2001.
- [2] ITU-T Recommendation G.709,
- [3] ITU-T Recommendation G.872, "Architecture of optical transport networks", February 1999