97A000183

RC-20716 (91807) 2/5/97
Computer Science/Mathematics 22 pages

Research Report

Automatic Fault Detection, Isolation, and Recovery in Transparent All-Optical Networks

Chung-Sheng Li, Rajiv Ramaswami
IBM Research Division
T.J. Watson Research Center
P.O. Box 218
Yorktown Heights, NY 10598

IBM Research Division
Almaden • T.J. Watson • Tokyo • Zurich • Austin

Automatic Fault Detection, Isolation, and Recovery in Transparent All-Optical Networks

Chung-Sheng Li and Rajiv Ramaswami*

IBM Thomas J. Watson Research Center
P.O. Box 704
Yorktown Heights, NY 10598
Telephone: (914) 784-6661, (914) 784-7356
Email: {csli,rajiv}@watson.ibm.com

December 9, 1996

Abstract

Network fault identification is an important network management function which is closely related to other network management functions such as fault management, configuration management, and performance management. This paper investigates fault surveillance and fault identification mechanisms for a transparent optical network in which data travels optically from the source node to the destination node without going through any optical-to-electrical (O/E) or electrical-to-optical (E/O) conversion. Mechanisms and algorithms are proposed to detect and isolate faults such as fiber cuts, laser, receiver, or router failures. These mechanisms allow non-intrusive device monitoring without requiring any prior knowledge of the actual protocols being used in the data transmission.

1 Introduction

Network management is essential to ensure efficient and continuous operation of any network. Network management functions include the management of configuration, faults,

---

*This work was funded in part by grant no. MDA 972-92-C-0075 from ARPA.

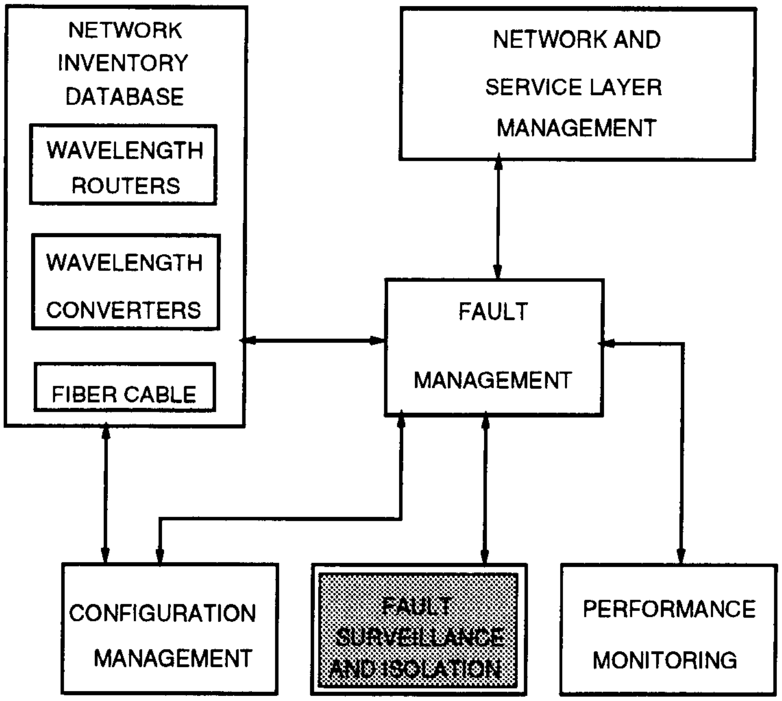


Figure 1: Relationship between fault surveillance/isolation and various components of network management.

performance, accounting and security [1], all of which are usually related to one another. The relationship between the various functional components of a network management layer is shown in Fig. 1. The most important component in this system is the fault surveillance system as it provides information for the fault management, configuration management, and the performance management systems. The fault surveillance modules are responsible for monitoring the operating condition of each component, detecting the loss-of-light condition for fiber optic links, reporting these fault conditions to the fault management unit(s). These unit(s) then analyze these fault conditions and use the information to update the network inventory database which contains entries for each of the components in the network. When a network component failure condition is detected, the fault isolation part of the fault management system determines the exact location of the fault(s).

Most of the fault-detection functions in current fault-management schemes are performed locally by an *agent*. The agent then communicates with a network management center using either the Simple Network Management Protocol (SNMP) or the Common Management Information Protocol from Open System Interconnection (OSI CMIP). These protocols enable the management platforms to query management information of heterogeneous multi-vendor devices in a uniform manner. In a *centralized* network management system, only one controller is active in performing the network management functions. In contrast, multiple controllers share the network management functions in a *distributed* network management

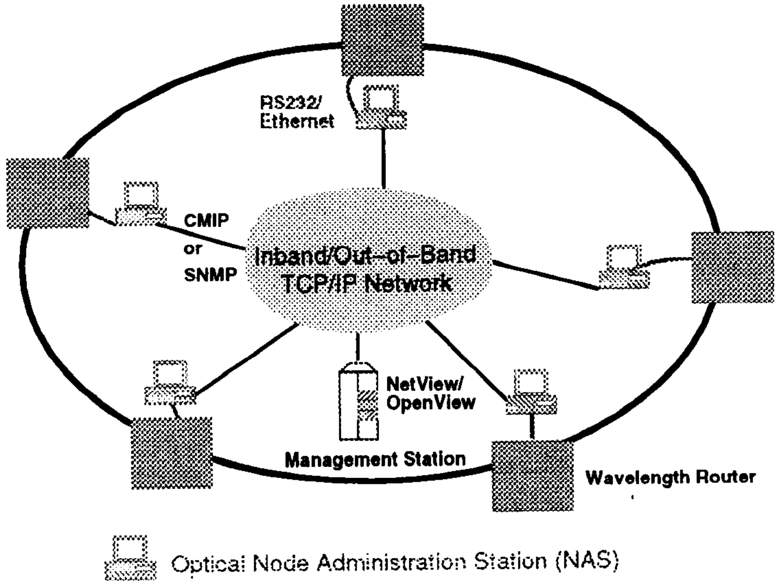


Figure 2: Network managment platform for an optical network.

system. A distributed network management system is usually more robust but is also more complicated in terms of maintaining the consistency of the network inventory database and distributed restoration of part or all of the network. A typical management platform that might apply to an optical network is shown in Fig. 2.

Recent network management studies [2, 3, 4, 5, 6] focus on management mechanisms for networks such as SONET/ATM (synchronous optical network/asynchronous transfer mode) networks. These networks consist of electronic switches interconnected by point-to-point optical fiber links.

In contrast to SONET/ATM networks, in an *all-optical network* [7, 8], data travels optically from source to destination without going through any optical-to-electronic (O/E) and electronic-to-optical (E/O) conversion. All-optical networks typically use optical wavelength division multiplexing (WDM) to harness the vast fiber bandwidth by breaking it up into several channels, each at a different wavelength operated at moderate electronic speeds to realize large overall network capacities. An important advantage of an all-optical network is that it is *protocol transparent*; in other words, once a connection is set up between two end nodes, the network does not impose any bit rate, frame format or other protocol limitations. Thus at any given time it is possible for several connections to exist, with each using a different protocol. This is attractive since a single physical infrastructure can be used to support multiple protocol streams. This transparency imposes a new requirement on the network management framework since the management mechanism (agent) may have no prior knowledge of the the protocols being used in the network. Furthermore, the agent may no longer have access to the overhead bits that are previously used to transport supervisory information between repeaters or switching sites to perform its management functions.

Therefore, new methods for fault detection and isolation and are necessary.

Only recently have researchers begun to consider management requirements for optical networks. Management requirements for transporting ATM cells over shared fiber passive optical networks with a passive optical tree and branch topology are discussed in [9, 11]. For long-haul optically-amplified systems, a separate supervisory channel using either an independent wavelength or a subcarrier channel is proposed in [13, 14, 15, 16, 17, 18, 19, 20] to isolate faults and to provide performance indicators. The implementation of a supervisory channel includes the use of an in-band or out-of-band WDM channel, pump modulation schemes, and counter-propagating methods [16]. For wavelength-routed networks, [10] proposed a supervisory system wherein an out-of-band pilot tone is added by each transmitter. This pilot tone provides signal identification and power level information for fault management at intermediate nodes without requiring the signal itself to be received and regenerated. The power level information is also used to equalize the powers of the different channels within each router.

This paper proposes fault detection and isolation mechanisms for (a) *broadcast-and-select* networks, and (b) *wavelength-routed* networks. These architectures are discussed in detail in Section 2. These mechanisms detect and isolate active component faults, fiber link cuts, and ensure that Federal eye-safety requirements (FDA regulation 21 CFR subchapter J, ANSI laser safety standard Z136.2, IEC Laser Safety Standard 825) are complied by shutting down the link when open fiber links are detected, and perform automatic link recovery when the links or devices have been repaired. This goal is achieved by using a supervisory channel, a concept generalized from [12, 13, 14, 15, 16, 17], to provided fault detection and isolation for each individual fiber segment between any two active devices (e.g., optical amplifiers, routers, wavelength translators, laser transmitters and receivers) and also to monitor the performance of the active devices in the network. The proposed supervisory system located at each active device acts as an agent and communicates with other agents and the fault management and configuration management functions through SNMP or CMIP to report device status and to receive control commands.

The ITU is currently in the process of setting standards for transmission systems and networks using optical amplifiers [30, 31]. It is expected that standardization efforts in the area of network management and fault isolation will follow soon.

The paper is organized as follows: Section 2 describes the network architectures that we consider. The failure modes of the components used in the network are discussed in Section 3 . Based on these failure modes, fault identification and isolation mechanisms for broadcast-and-select networks and wavelength-routed networks are investigated in Section 4 and Section 5, respectively. A summary of the paper appears in the last section.

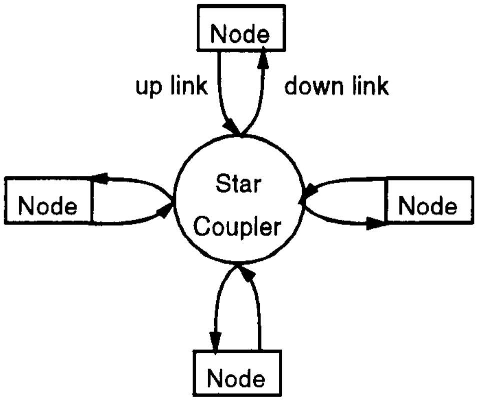


Figure 3: A broadcast-and-select network.

2 Network Architectures

2.1 Broadcast-and-Select Networks

A broadcast-and-select network consists of nodes interconnected to each other via a star coupler, as shown in Fig. 3. An optical fiber link, called the *uplink*, carries signals from each node to the star. The star combines the signals from all the nodes and distributes the resulting optical signal equally among all its outputs. Another optical fiber link, called the *downlink*, carries the combined signal from an output of the star to each node. Examples of such networks are Lambdanet [21] and Rainbow [22].

2.2 Wavelength-Routed Networks

A wavelength-routed network is shown in Fig. 4. The network consists of *static* or *reconfigurable* wavelength routers interconnected by fiber links. Static routers provide a fixed, non-reconfigurable routing pattern. A reconfigurable router on the other hand allows the routing pattern to be changed dynamically. These routers provide static or reconfigurable *lightpaths* between end-nodes. A lightpath is a connection consisting of a path in the network between the two nodes and a wavelength assigned on the path. End-nodes are attached to the wavelength routers. One or more controllers that performs the network management functions are attached to the end node(s).

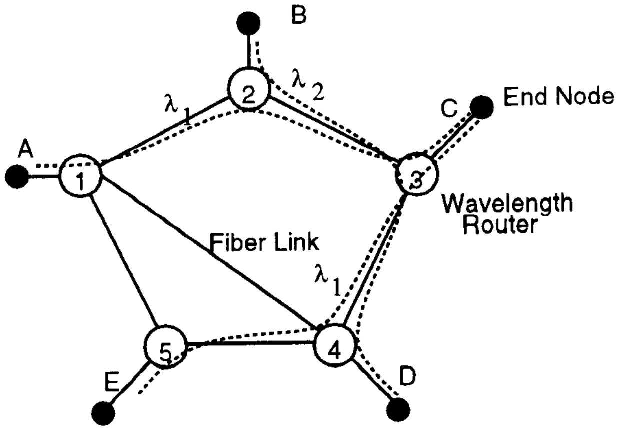


Figure 4: A wavelength-routed network.

3 Network Failure Modes

We next list the set of possible faults in a transparent all-optical network. We consider only the failure modes for active components in the network (transmitters, receivers, switches, optical amplifiers) and assume that the packaged passive components (couplers, gratings) are reliable. The active components are usually telecom grade and by themselves have fairly long mean-time-between-failures of several years.

(1) Optical fiber fault: This occurs when a fiber segment is cut. Means for monitoring and detecting this will be discussed in Sections 4 and 5.

(2) Transmitter fault: This occurs when a tunable or fixed-tuned laser, its monitor photodiode, or its driver circuitry used at the transmitter fails. This can be sensed in two ways: first a monitor photodiode is packaged along with the laser. The photodiode detects the light output from the back facet of the laser and this signal can be used to control the laser bias and modulation currents. In addition, the laser driver senses the bias current of the laser diode and triggers a threshold crossing alert (TCA) if it is not within normal limits.

(3) Receiver fault: This could occur due to the malfunction of the tunable or fixed-tuned filter, the optical receiver, the servo mechanism for stabilizing the wavelength reception, or the timing recovery circuitry. We will assume that each receiver is provided with a separate light detector at its input. If the detector detects light when the receiver does not provide a signal current output, then we can establish that the receiver has failed.

(4) Optical amplifier fault: This usually arises from loss of signal, fuse or power circuit failures, pump laser(s) failure, input signal monitor failure, amplifier optical path failure (i.e., fiber break or passive component failure within the amplifier), or optical surveillance channel failure [17]. Means for monitoring and detecting this will be discussed in Section 5.

(5) Wavelength router fault: In this paper, we only consider fault monitoring mechanisms for

reconfigurable wavelength routers. A *static* wavelength router [23, 8] consists only of passive devices such as grating demultiplexers and multiplexers or phased arrays. These devices are considered reliable and their failure mechanisms will not be discussed here. Reconfigurable routers [24, 8] have active switching elements within them and are more useful for networks. These routers can be realized using a combination of optical demultiplexers, switches and multiplexers, or by using acoustooptic filters. The cause of failures of these routers could be due to the failure of the switches/acoustooptic filters, loss of signals, fuse or power circuit failure, and optical path failure. and multiplexers, modes are not considered here. Means for monitoring and detecting these faults will also be discussed in Section 5.

(6) Wavelength converter fault: Wavelength converters usually consist of semiconductor optical amplifiers or distributed Bragg reflector lasers based on saturable absorption [25, 26]. The cause of the failures of these wavelength converters could arise from the failure of the saturable absorber, the loss of signal, the fuse or power circuit failure, and the optical path failure. Means for monitoring and detecting converter failures will be discussed in Section 5.

4 Fault Management in Broadcast-and-Select Networks

A point-to-point link between two nodes A and B is shown in Fig. 5. The current practice of managing the link is as follows. (See for example, the Fiber Channel Standard [27].) Each transceiver could be in any of the four states: ACTIVE, DISCONNECT, STOP, and RECONNECT. Under normal circumstances a node is in the active state when the transceiver is sending and receiving data. Assume both node A and B are in the active state. If the fiber $A \rightarrow B$ is cut, Station B detects a loss of light on that link with its receiver, turns off its laser transmitter and enters into the disconnect state. Station A then detects loss of light, turns off its laser transmitter and enters into the disconnect state. Thus no light emanates from the cut fiber and the eye-safety regulations are satisfied.

In order to bring the link back up once it is repaired, the following ON-OFF-ON reconnect protocol is conducted between node A and B. Station A and B both periodically pulse their laser transmitters while in the disconnect state. This pulsing results in an average optical power on the link that is less than that allowed by eye-safety regulations. In this instance once the fiber $A \rightarrow B$ is repaired, Station B's monitor detects these pulses and its laser transmitter responds to node A. A and B then enter the STOP state where they both stop sending pulses. If no light is detected for a certain time period each node enters the RECONNECT state where it periodically pulses its lasers. Now, upon detecting light at its receiver, the node goes back into the ACTIVE state. The intermediate STOP state is required in order to prevent the tranceiver from entering the ACTIVE state as a result of connecting to the wrong fiber and to ensure that both ends comply with the safety mechanism.

Extending this approach to a multipoint-to-multipoint star network of Fig. 3 does not appear to be straightforward. First there is the problem of determining the exact location of

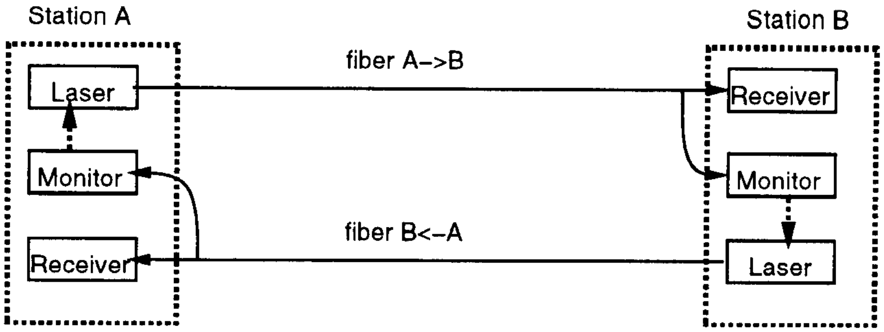


Figure 5: Managing link failures in a point-to-point link.

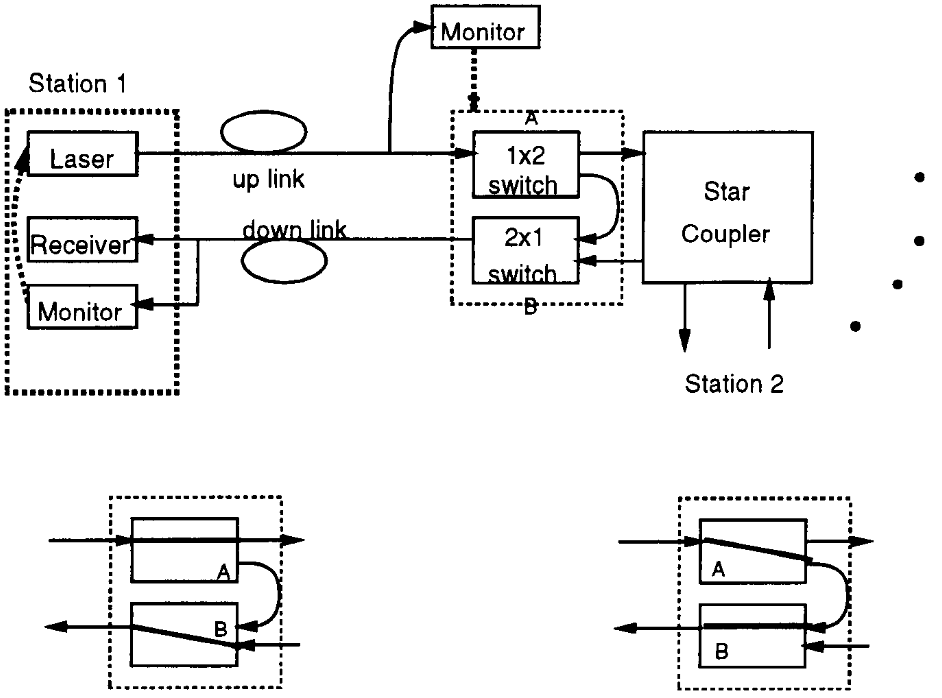
a failure. For instance if an uplink from node X fails, all nodes including X will still detect the presence of light on all of their downlinks. Another instance of a failure is when the downlink to node X fails. In this case node X can easily detect the absence of light and determine that the downlink has failed. However other nodes will not be aware of this fact and will continue to transmit. This will result in the violation of the eye-safety regulations on the failed down link. Moreover, it is undesirable to have other nodes stop transmission altogether while this link is in the failed state.

We now propose a link monitoring scheme that detects the operating condition of each link in a star network, takes it down once a link cut is detected, keeps the optical power levels on cut links within eye-safety limits, automatically brings the link back up once the cut is restored, all the while not affecting the operation of the other nodes in the network except the node whose link is cut. This scheme achieves these objectives by providing each node with an optical bypass switch located at the input/output ports of a star coupler, along with a means to detect the presence or absence of light on an uplink at the star and on a downlink at the node.

Fig. 6 shows the configuration for a particular node, node 1, in the network and its connections to a star coupler via a pair of uplink and downlink. In addition to the monitor photodiode provided at the transceiver, a bypass module, also shown in Fig. 6, is located at the input/output port of the star coupler so that a portion of the power coming in on the uplink is tapped off and monitored by a photodiode. This photodiode detects the presence or absence of light on the link and its output is used to drive a finite state machine (Fig. 7) which keep tracks of the current state of the link.

For simplicity we will describe the procedure used for a particular node, node 1. The same procedure is used independently for each node in the network.

Hardware finite state machines (FSMs) are used to keep track of the current state of each link, within the end node, FSM-N, as well as in the bypass module, FSM-B. Fig. 7 shows the FSM used at the node and Fig. 8 shows the FSM used at the bypass module. In the normal mode of operation, both the end node and the bypass module are in the ACTIVE



Normal Operation

Loop Back when failure is detected

Figure 6: Managing link failures in an optical star network.

state. While in this state, optical switch A of the bypass module is set in the "bar" position allowing light from node 1 to go into the star coupler. Optical switch B is set in the "cross" position allowing light from the star coupler to be received by node 1. In this configuration, the bypass module is transparent to the network operations.

If the uplink fails, the monitor photodiode at the bypass module detects the loss of light, enters into the DISCONNECT state, sets switch A in the "cross" position and switch B in the "bar" position. In this *loopback* configuration, the uplink is connected to the downlink so that node 1's transmitter is connected to its receiver. This causes the node to see a loss of light and enter into the DISCONNECT state.

If the downlink fails, the node detects loss of light using its monitor photodiode, enters into the DISCONNECT state and turns off its transmitter. This causes the bypass module to see a loss of light and enter into the DISCONNECT state.

Therefore once either the uplink or downlink fails, the node's transmitter is turned off and the optical switches are set in the loopback position and both the node and bypass module enter the DISCONNECT state.

Note that in principle, if the uplink fails and the downlink is still up, we could leave the downlink connected to the star and the node can continue to receive data. However we

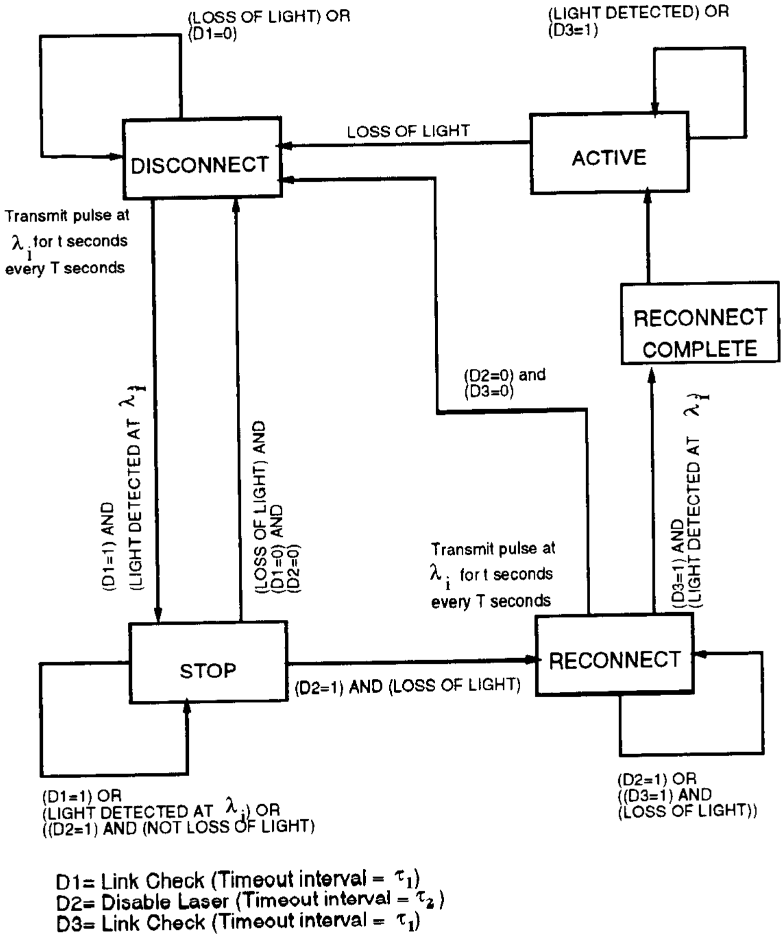


Figure 7: Fault detection and recovery finite state machine at the node.

cannot then detect the failure of the downlink at the star at a later point in time. Thus we disconnect the downlink from the star in this event.

Based on the above we have the following property:

Property 1: *If either the uplink or the downlink is cut, both FSM-N and FSM-B enter the DISCONNECT state and no light is transmitted over the broken links.*

While in the DISCONNECT state the node periodically sends light pulses (t seconds for every T seconds) as in the standard procedure for point-to-point links. When the failed link is repaired (either the uplink or downlink or both), the node can then receive its own pulses and goes through the STOP state and the RECONNECT state to confirm that the link is up (see Fig. 7 for details). Similar to the point-to-point link case described earlier, an ON-OFF-ON protocol is required in order to avoid accidental entry into the active state due to incorrect fiber connections. When the RECONNECT state is reached, both the node and the bypass module enter into the RECONNECT COMPLETE state for a short period

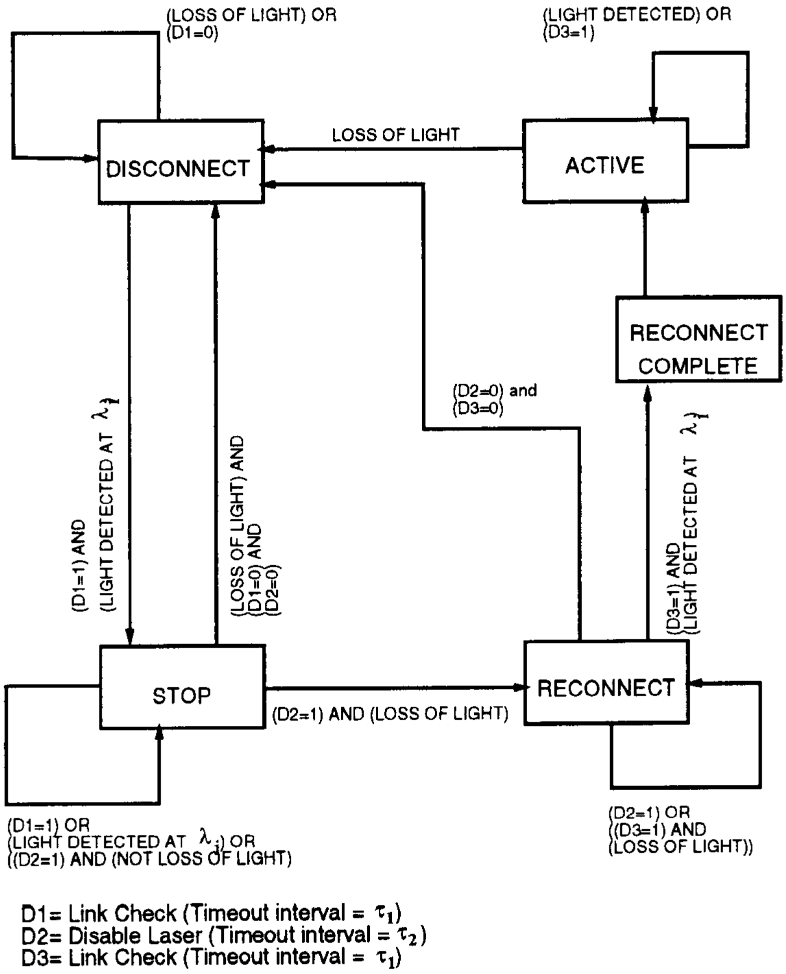


Figure 8: Fault detection and recovery finite state machine at the bypass module.

of time to allow the resetting of the switches before resuming normal operations.

Note that the loopback of the uplink and downlink achieves two functions: (1) it allows the node to determine for itself when the link comes back up, (2) more importantly it allows other nodes in the network to continue transmission without being interrupted. A major problem in the broadcast network is that if a downlink goes down, although that corresponding node can stop transmitting, there is still power coming on to the failed link from other nodes in the network. This is prevented by looping back the up and down links as shown in Fig. 6.

Note that there exists a monitor photodiode in front of the receiver, so that the receiver failure condition can be distinguished from link failures. However, isolation of the monitor photodiode failures at either the end node or the bypass module from the switch failures and the fiber link failures is not possible in this implementation. Once a loss-of-signal condition is indicated at either the end node or the bypass module, the switch will be put in the loopback mode and the transmitter at the end node which is affected enters into the pulsing mode until the failure is repaired. Using two photodiodes at each monitor photodiode position, however, could reduce the probability of photodetector failure. In this case, a loss-of-signal condition is recognized only if *both* of the photodetectors do not receive optical signals.

While in the DISCONNECT state, the node sends pulses of width t and period T. Upon receiving a pulse of width t, FSM-N enters the STOP state. Upon receiving a pulse of width t, FSM-B also enters the STOP state. In the STOP state, the node stops transmission. If no light is detected for a time period τ_1, then FSM-N enters the RECONNECT state. At the bypass module, in the STOP state, if no light is detected for a time period τ_1, then FSM-B enters the RECONNECT state. If light is detected within this time period τ_1 then the FSMs return to the DISCONNECT state. Upon entering the RECONNECT state the node again sends pulse of width t and period T. Upon receiving a pulse of width t within a duration τ_2, FSM-N enters the RECONNECT COMPLETE state, otherwise it goes back to the DISCONNECT state. Upon receiving a pulse of width t within a duration τ_2, FSM-B also enters the RECONNECT COMPLETE state, otherwise it goes back to the DISCONNECT state. The FSMs remain the RECONNECT COMPLETE state for a fixed duration τ' during which the bypass module resets its switches to connect the node to the star, after which both enter the ACTIVE state. The time periods t, T, τ_1 and τ_2 must be chosen carefully with $\tau_1 + \tau_2 < T - t$.

In order to better understand the restoration procedure and to informally prove the correctness of the FSMs, consider the following cases:

Case 1: The uplink has been cut while the downlink has not been cut. Both FSMs have entered the DISCONNECT state.

Until the uplink is restored, both FSMs remain in the DISCONNECT state. Once the uplink is restored, FSM-B enters the STOP state, followed shortly by FSM-N. The node now stops transmitting. Both ends now detect a loss of light and enter the RECONNECT state. The node now starts transmitting, causing both ends to enter the RECONNECT COMPLETE state and eventually the ACTIVE state.

Case 2: The downlink has been cut while the uplink has not been cut. Both FSMs have entered the DISCONNECT state.

In this case until the downlink is restored, FSM-N remains in the DISCONNECT state. FSM-B howevers proceeds to the STOP state (when it sees the pulsing of light from the node) and then to the RECONNECT state (when the pulsing stops). In the RECONNECT state however, it does not see light within a period τ_2 and hence returns to the DISCONNECT state. FSM-B shuttles between these three states until the downlink is restored. Once the downlink is restored, FSM-N enters the STOP state and the node stops transmitting pulses and enters into the RECONNECT state after a time τ_1. FSM-B also enters the STOP state and then the RECONNECT state after a time τ_1. The node now starts transmitting and both FSMs enter the RECONNECT complete state and then the ACTIVE state.

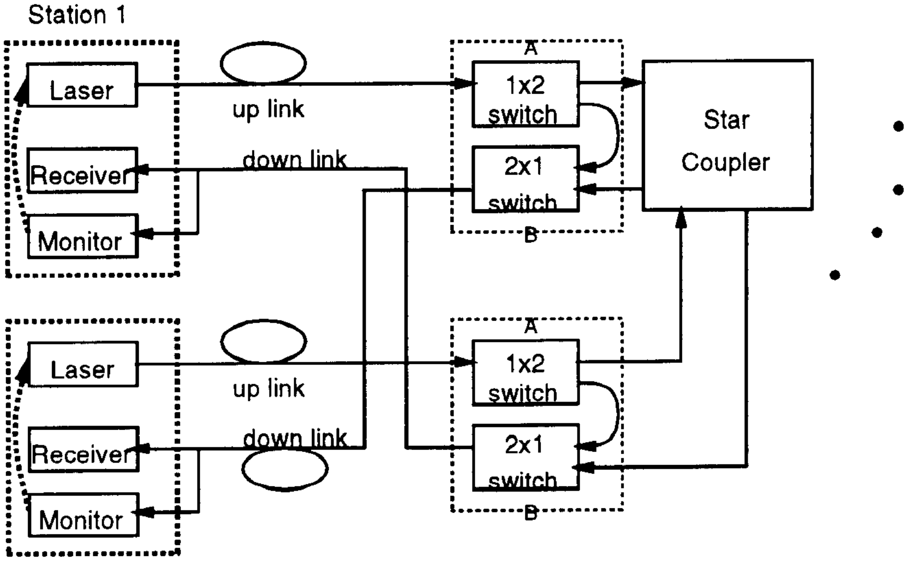


Figure 9: Incorrect fiber connections in a star network.

Case 3: Both uplink and downlink are cut. In this case both FSMs remain in the DISCONNECT state until one of the links is restored after which they follow Case 1 or 2. The case when both links are restored simultaneously is similar to Case 1.

Case 4: Incorrect fiber connections: An interesting case is when links between two nodes and the star get cut and they happen to get wired incorrectly when they are restored, as shown in Fig. 9. In this case the two nodes are directly connected to each other. If the two nodes receive on the same wavelength then they will enter the ACTIVE state along with the two bypass modules after which the situation is as shown in Fig. 9. Normal operation is restored despite the incorrect wiring. If the receivers in the two nodes are tuned to their transmit wavelengths and the two wavelengths are different, then both nodes will remain in DISCONNECT state while their bypass modules shuttle between the DISCONNECT, STOP and RECONNECT states.

Based on the informal descriptions above we infer the following property:

Property 2: *Once an uplink or downlink failure has been restored, both FSM-N and FSM-B enter the ACTIVE state.*

5 Fault Management in Wavelength-Routed Networks

We assume that one wavelength λ_0 will be used to carry signals intended for network management. The concept of using a dedicated wavelength as a supervisory channel for long-haul communications has been proposed previously, for example, in [17]. In this paper, this concept is generalized to include other network components such as wavelength routers and wavelength converters. Furthermore, architectures and protocols are proposed to shutdown the active optical devices and block the optical path whenever there is a potential danger of violating eye safety requirements and recover the link automatically when the faults are repaired.

The supervisory wavelength can also be used for network control, as described in [28]. In the scheme proposed in this section, each active device (optical amplifier, wavelength router and wavelength converter) has a fault surveillance controller. The supervisory wavelength channel is used to establish lightpaths between all adjacent pairs of controllers. On top of this control architecture we assume the existence of a distributed algorithm that conveys management updates to a centralized controller or to distributed controllers that are in charge of fault isolation.

5.1 Link and Amplifier Faults

Under normal operation, the controllers at the ends of a link communicate on λ_0 and monitor this continuously to determine the presence or absence of light. Now we treat the situations where a cut occurs along a segment of this link or one of the amplifiers on the link fails. In this event the transceivers at the ends of the lightpaths using the link detect a loss of light condition and then execute the procedure described in Section 4 to bring the lightpaths back up after the link is restored. This is done for all wavelengths except one (λ_0), which is treated in a special manner, as described below.

We assume that the fiber amplifiers are always installed in pairs. The proposed fault monitoring and isolation mechanism for each pair of optical amplifiers is shown in Fig. 10. In this figure, i is an amplifier stage while $i-1$ and $i+1$ could be an end node, another amplifier stage, or a wavelength router. At the input to the amplifier, the control signal at wavelength λ_0 is completely tapped off, received, and converted to an electrical signal. This can be done by a wavelength-selective coupler, and is particularly easy if λ_0 is spaced apart from the other wavelengths, for example at 1.3μ with the other wavelengths being in the 1.5μ window. Under normal operation this signal is electrically switched and remodulated onto a laser at λ_0 and combined back at the output of the amplifier using another wavelength-selective coupler. The received signal is also fed to the fault processing unit. Under normal operation, the unit is in the active state (see Fig. 11) and simply passes the signal through. onto a laser at onward procedure is used in the reverse direction as well.

The operation of the two segments AB and CD is controlled by a main state machine shown in Fig. 11 that resides in the fault processing unit. This state machine in turn controls two state machines, one for segment AB and another for segment CD. If a loss-of-light condition on one of the links, say link AB in Fig. 10 is detected, the fault processing unit enters into the AB-Fail state and the λ_0 signals in both directions are terminated in the fault processing unit. The unit then generates a new signal indicating a fault and sends

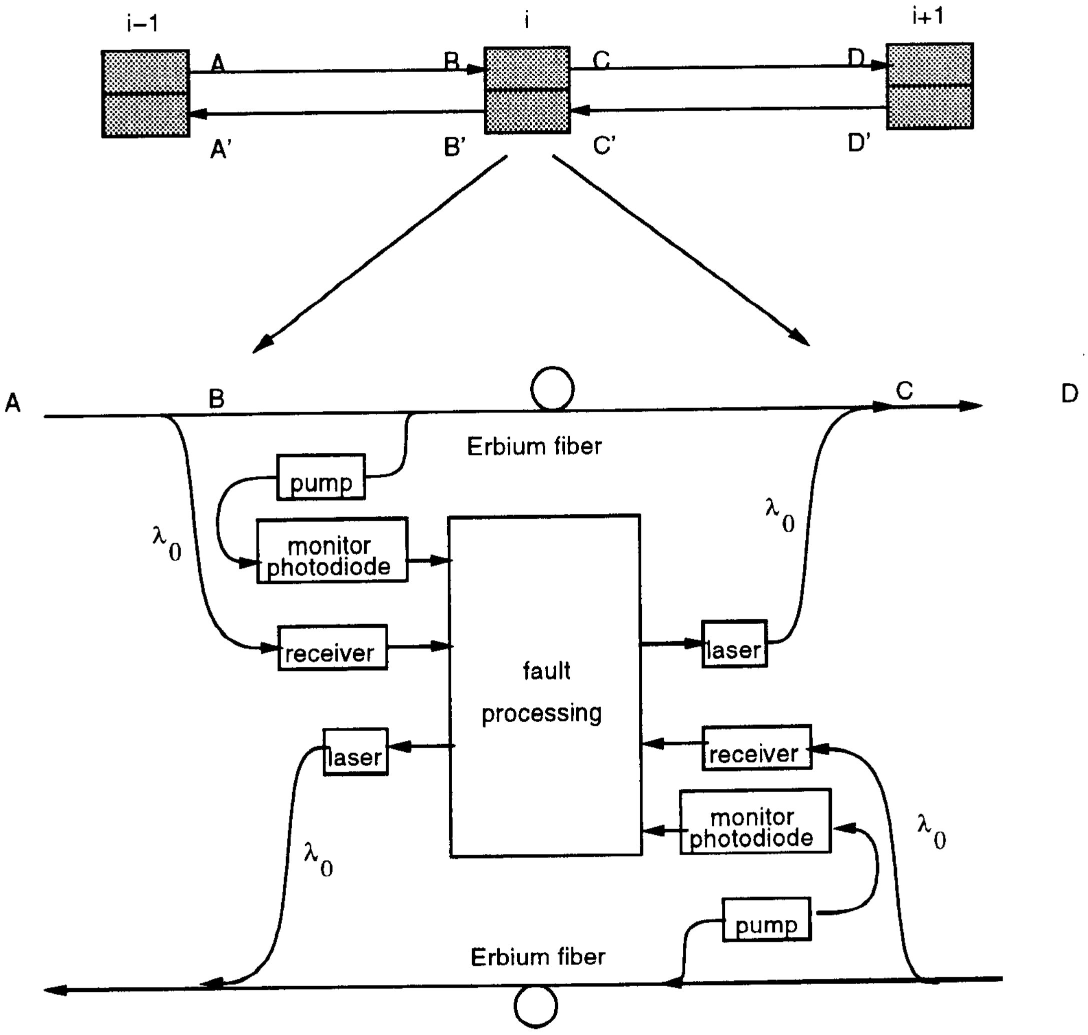


Figure 10: Fault management structure for link segments and optical amplifiers.

it on link CD. This enables the controller at the adjacent node D to determine the location and type of the failure. The transmitters at either end of AB then go into the the disconnect state (as described in Fig. 7 and Fig. 8). When the link is repaired, the transceivers at both ends of link AB go through the stop and reconnect states before resuming normal operation.

If a loss of light is detected on both of AB and CD simultaneously, the fault processing unit enters into the *isolate* state. In this case, the fault processing unit cannot send out any information since both AB and CD are down. However, the state machines controlling segment AB and CD continue to operate trying to bring the segments back up. Once a segment is up again, the main state machine enters state AB-FAIL (if CD comes back up) or state CD-FAIL (if AB comes back up). At this point the fault processing unit can propagate the information to other processing units on the links.

A second photodiode is used to monitor the scattered light from the pump laser. If the photodiode indicates that the pump laser has failed, the fault controller interrupts the λ_0 signal in both directions and interposes a message indicating this fact. When the pump laser is replaced, the photodiode detects the presence of light and normal operation is restored. Since there is no danger of leaking laser light, neither of the transceivers at A or D will enter into the pulsing mode. The link will continue to operate using one wavelength (λ_0). The other lightpaths using the link will be taken down due to the loss-of-light detection at their endpoints.

A third photodiode is used to monitor the output of the amplified optical signals. This monitoring is necessary to discover the optical path failure condition within the optical amplifier. If the photodiode indicates that the internal optical path has failed, the fault controller interrupts the λ_0 signal in both directions and interposes a message indicating this fact. When the internal optical path is repaired, the photodiode detects the presence of light and normal operation is restored. Since there is no danger of leaking laser light, neither of the transceivers at A or D will enter into the pulsing mode. The link will continue to operate using one wavelength (λ_0). The other lightpaths using the link will be taken down due to the loss-of-light detection at their endpoints.

If multiple segments along a link fail simultaneously, the controller at one end of the link first obtains the location of the failed segment closest to it. Once this segment is back up, it is then able to determine the location of the next failed segment and so on. The two controllers at the ends of the link can thus work their way in starting from the ends of the link to identify in sequence a set of failed segments.

The failure of any of the monitor photodiodes is treated as loss-of-signal condition. Similar to the situation in a broadcast-and-select network, dual monitor photodiodes can be used to distinguish between monitor failure and optical link failure.

5.2 Router Faults

Detecting a fault inside a wavelength router is somewhat complex. The detection mechanism also depends on the internal structure of the router. We consider only the router structure in Fig. 12 and assume that the only components that fail are the optical switches, one of which is present for each wavelength.

If a switch fails, at least one of the lightpaths flowing through the switch will be affected. This will result in a loss of light condition being detected at the ends of the lightpath. The end nodes then communicate with each node along the path of that lightpath to determine whether it is a link failure. If it is not a link failure, then the next step is to determine the switch that has failed. The mechanism to determine this fault must be as non-intrusive as possible, i.e., other lightpaths must not be affected.

We list two approaches that can be used to identify a switch fault. Both approaches

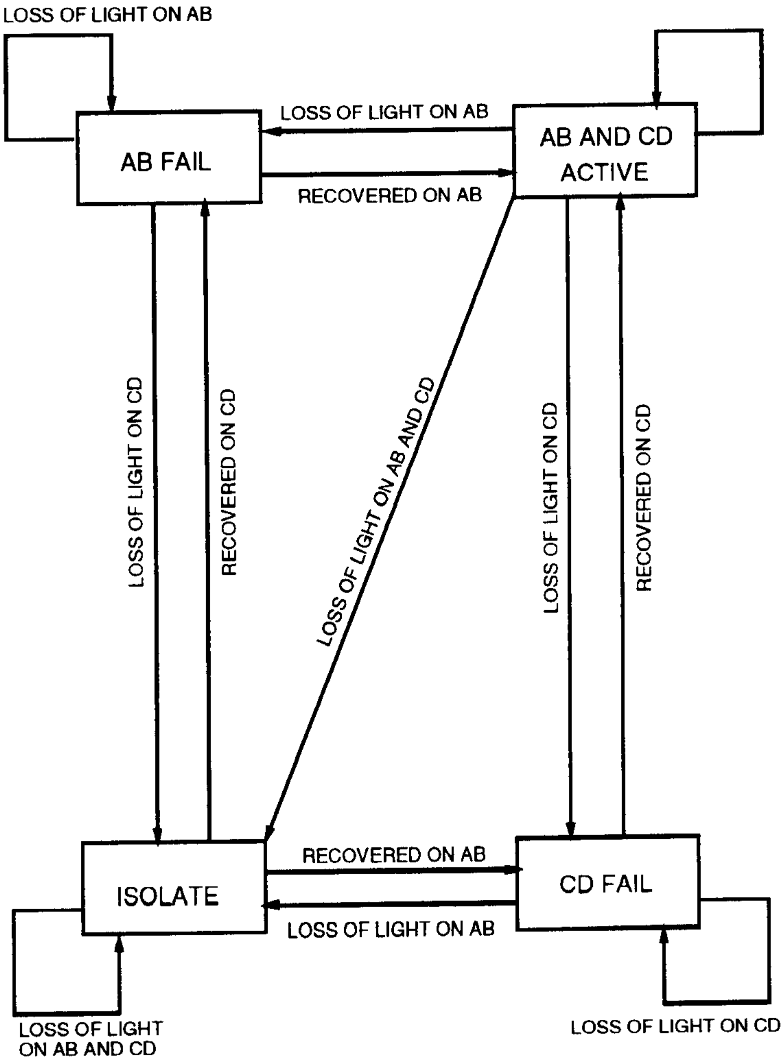


Figure 11: Fault testing and identification finite state machine.

require a local controller to be able to monitor the output from each switch port by using a monitor photodiode, as shown in Fig. 12. Thus each router must be provided with MN monitor photodiodes, where M is the number of ports and N the number of wavelengths per port.

The failed lightpath can be represented as a path in the network as shown in Fig. 13(a). Within each router along the path, we have shown only the switches used by the lightpath.

A. Local test signal injection and monitoring: For each switch along the route of the lightpath that has failed, the local controller injects a test signal at the corresponding switch input as shown in Fig. 13(b) and determines whether it is detected at the output of the switch, as suggested in [29]. Note that this signal must not be allowed to propagate further down

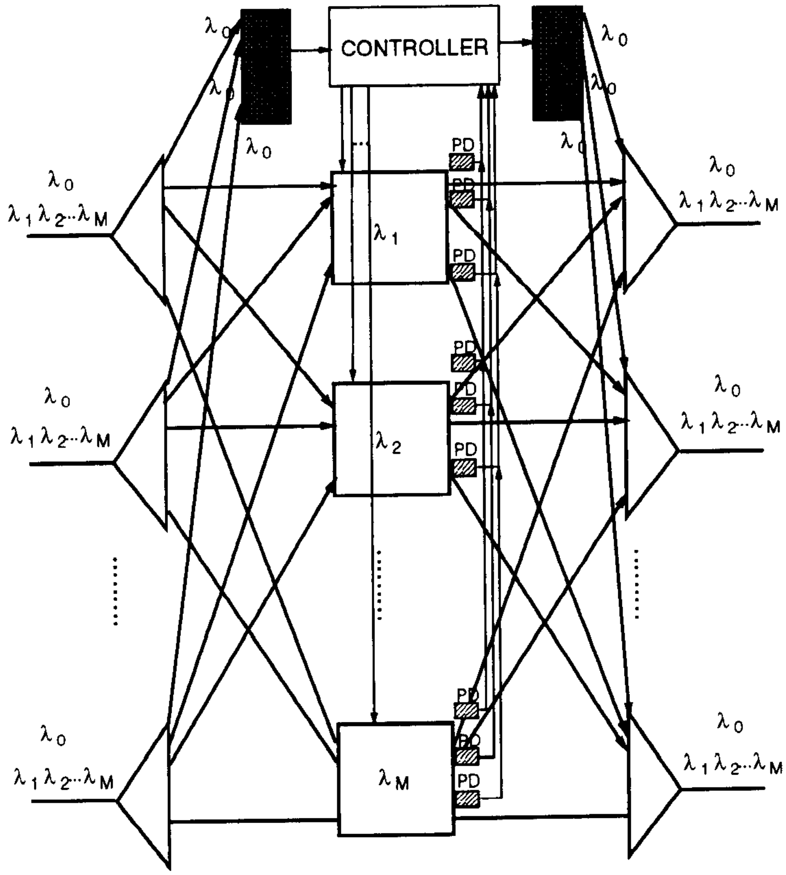


Figure 12: Error monitoring mechanism for wavelength routers.

the path. This is entirely non-intrusive and is the fastest way to locate the fault. However this requires each router to be provided with MN lasers in addition to the MN monitor photodiodes and may not be cost-effective.

B. End-node test signal injection with local monitoring: A better approach is to have the test signal generated and transmitted by the end node of the lightpath that has failed, while the monitoring is performed at the output of each switch by a monitor photodiode as shown in Fig. 13(c). If light is detected by the monitor on the $i-1^{th}$ node in the path and no light is detected by the monitor on the i^{th} node, then the switch at the i^{th} node has failed. The controllers along the path communicate with each other to determine the fault location using this procedure. This approach requires MN photodetectors for each wavelength router but no lasers and is also entirely non-intrusive but may not be as fast as the previous approach in identifying the failed switch.

Note that the approach detects the earliest fault in the chain. Successive faults can be detected in sequence after replacing the first failed switch.

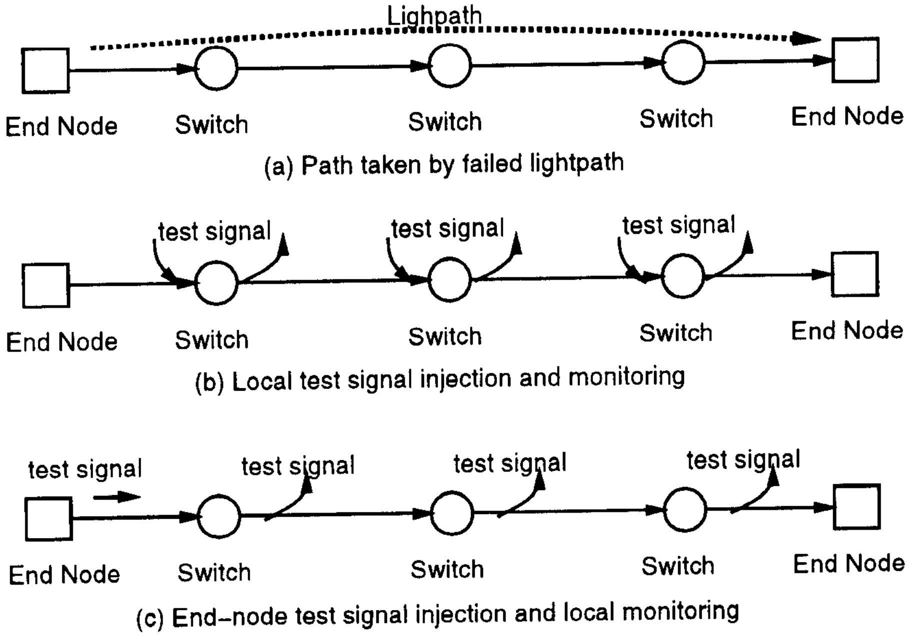


Figure 13: Fault testing and identification mechanism for failed switches

5.3 Wavelength Converter Faults

Similar to the amplifier case, we assume that the wavelength converters are always installed in pairs. Fault detection in a wavelength converter can be achieved by detecting the existence of optical signals at the desired wavelength. The supervisory wavelength is completely tapped off at the input and detected by a monitor photodiode, and produces a monitor current, A. An optical filter selecting the desired output wavelength bands is usually present at the output of the wavelength converter. A second monitoring photodiode is placed at the the output of the converter to detect the presence of valid output signals and produces a monitor current, B. A converter faulty condition can thus be detected when A is present but B is not present.

The fault monitoring and isolation mechanism for a converter placed in the middle of a link is identical to the mechanism proposed for optical amplifiers in Section 5.1. If the converter is within a wavelength router the fault detection and isolation can be performed by the controller attached to the router.

6 Summary

This paper proposed mechanisms to detect and isolate faults in transparent all-optical networks. Specific schemes were proposed for managing link faults in broadcast-and-select networks and wavelength-routed networks, and amplifier and router faults in wavelength-routed networks. These schemes may be useful for standardization efforts just beginning on network control and management of optical networks.

References

[1] S. Aidarous and T. Plevyak, "Telecommunication network management into the 21st century," IEEE Press, New York, 1994.

[2] J. E. Jakubson, "Managing SONET Networks," IEEE LTS, vol. 2, no. 4, pp.5-13, Nov., 1991.

[3] G. M. Berkowitz, P. T. Fuhrer, B. E. Gray, A. R. Johnston, and G. L. McElvany, "A nodal operations manager for SONET OAM&P," Proc. IFIP, pp. 403-411, 1991.

[4] S. Kheradpir, A. Gersht, W. Stinson, "Performance management in SONET based multi service networks," Proc. GLOBECOM'91, pp. 1406-1411, 1991.

[5] O. Tabata, T. Nishida, K. Sumal, "High speed management network for SONET based network," Proc. ICC'91, pp. 39-44, 1991.

[6] G. May and D. Jammu, "A distributed architecture for survivable SONET transport networks," Proc. GLOBECOM'91, pp. 2013-2017, 1991.

[7] "Special Issue on Broadband Optical Networks," IEEE Journal of Lightwave Technology, vol. 11, no. 5/6, May/June, 1993.

[8] R. Ramaswami, "Multiwavelength lightwave networks for computer communication," IEEE Communication Magazine, vol. 31, no. 2, pp. 78-88, Feb. 1993.

[9] J. Sanchez, S. Glick, Q. Sham, L. Sara, and L. Cuthbert, "Management requirements of a passive access network," Proc. SPIE, vol. 1974, pp.281-292, 1993.

[10] G. R. Hill et al, "A Transport Network Layer Based on Optical Network Elements," IEEE JLT, vol. 11, no.5-6, pp. 667-679, May/June, 1993.

[11] C.-S. Li and R. Ramaswami, "Network Management for Protocol-Transparent Broadcast-and-select Networks," to be presented in ICC'95 Workshop on WDM Optical Network Management and Control, June, 1995.

[12] C.-S. Li and R. Ramaswami, "Fault Detection and Isolation in Transparent All-Optical Networks," submitted to GLOBECOM'95.

[13] J. E. Talor, "Maintenence and Telemetry Overview of Optically Amplified Systems," OFC'95 Workshops on OAM&P in Lighwave Systems Using Optical Amplifiers, Feb. 1995.

[14] Y. Tada, "OAM&P for High-Speed Optical Terrestrial Networks Applying Optical Line Amplifiers and for Next Generation Lightwave Networks," OFC'95 Workshops on OAM&P in Lighwave Systems Using Optical Amplifiers, Feb. 1995.

[15] C. Konishi, "Supervisory Signal Transmission Scheme by Pump LD Modulation for EDFA Repeater System," OFC'95 Workshops on OAM&P in Lighwave Systems Using Optical Amplifiers, Feb. 1995.

[16] J. A. Nagel, "Telemetry System for Long Haul Terrestrial Optically Amplified Lightwave Systems," OFC'95 Workshops on OAM&P in Lighwave Systems Using Optical Amplifiers, Feb. 1995.

[17] P. Bonenfant, "OAM&P For Single and Multiwavelength Lightwave Systems Using Optical Amplifiers," OFC'95 Workshops on OAM&P in Lighwave Systems Using Optical Amplifiers, Feb. 1995.

[18] S. F. Habiby, K. Bala, P. A. Bonenfant, C. J. Byrne, and R. S. Vodhanel, "Network Management Challenges for Multi-wavelength Optical Networks," ICC'95 Workshop on WDM Optical Network Management and Control, June, 1995.

[19] S. Okamoto, N. Nagatsu, M. Koga, and K.-I. Sato, "Management Concepts of Optical Path Networks," ICC'95 Workshop on WDM Optical Network Management and Control, June, 1995.

[20] R. E. Tench, "Control, Telemetry and Performance Monitoring in WDM Lightwave Systems Using OAs," ICC'95 Workshop on WDM Optical Network Management and Control, June, 1995.

[21] M. S. Goodman, H. Kobrinski, M. Vecchi, R. M. Bulley and J. M. Gimlett, "The LAMBDANET multiwavelength network: architecture, applications and demonstrations," IEEE J. Selected Areas in Commun., vol. 8, no. 6, Aug. 1990, pp. 995-1004.

[22] F. J. Janniello, R. Ramaswami and D. G. Steinberg, "A prototype circuit-switched multi-wavelength optical metropolitan-area network," IEEE/OSA J. Lightwave Tech., vol. 11, May/June 1993, pp. 777-782.

[23] C. Dragone et al., "Integrated optics $N \times N$ multiplexer on Silicon", IEEE Photonics Tech. Lett., vol. 3, Oct. 1991, pp. 896–899.

[24] C. A. Brackett et al., "A scalable multiwavelength multihop optical network: a proposal for research on all-optical networks", IEEE/OSA J. Lightwave Tech., May/June 1993, pp. 736–753.

[25] A. Paradisi and I. Montrosset, "Analysis of wavelength conversion using a multisection DBR laser with a saturable absorber," IEEE Journal of Quantum Electronics, vol. 29, no. 5, May 1993, 1285-1294.

[26] S. Dubovitsky, P. D. Dapkus, A. Mathur, and W.H. Steier, "Wavelength conversion in a qunatum well polarization insensitive amplifier," IEEE Photonics Technical Letters, vol. 6, no. 7, July 1994, pp. 804-807.

[27] ANSI X3T9.3, "Open-Fiber-Control Protocol" in the Fiber Channel Standard, Annex I, FC-PH 4.3, 1994.

[28] R. Ramaswami and A. Segall, "Network control for wavelength-routing optical networks," Submitted to INFOCOM'96.

[29] Y.-W. Leung, "On-line fault identification in multistage interconnection networks," Parallel computing, vol. 19, pp.693-702, 1993.

[30] Draft Rec. G.mcs: Optical interfaces for multichannel systems with optical amplifiers, ITU-T, 1995.

[31] Draft Rec. G.lon: Functional characteristics of interoffice and long-haul line systems using optical amplifiers, including optical multiplexing", ITU-T SG 15/WP 4, 1995.