ISSN: 2277-3754
ISO 9001:2008 Certified
International Journal of Engineering and Innovative Technology (IJEIT)
Volume 5, Issue 4, October 2015

Optical Ethernet and its Survivability: A Comprehensive Survey

Lizzie D'cruz, Lecturer (SG), DBRAIT, Port Blair, Andamans

Abstract*— In the modern world, the data transfer from one place to another takes place at high speed, at the same time has good reliability with being secure. The advancements in Ethernet technology make the network simple and flexible to the changing traffic conditions. Optical communication is used in areas where high speed data transfer has to take place. Optical Ethernet is a new emerging technology which has used the features of Optics and Ethernet together for efficient data transfer from one end to another. The idea of combining the properties of Ethernet like flexibility and simplicity along with the features of Optics such as speed and reliability has resulted in the introduction of Optical Ethernet. Any failure in data communication may result in enormous data loss in the communication service. Nowadays, no network is made without proper restoration techniques in order to have, no loss of information. This paper aims to provide the details of Ethernet evolution, the building blocks of optical Ethernet and various research work done on the protection and restoration techniques for the survivability of optical Ethernet.

Index Terms—**Ethernet, survivability, virtual LAN, Spanning tree, Resilient Packet Ring & Dense wavelength division multiplexing.**

I. INTRODUCTION

Data communication from one place to another with high speed and reliability is the requirement of the modern world and any error in high speed data transfer even for a fraction of second may result in enormous data loss and an interrupted data is obtained at the receiver. Network with optical Ethernet can have the link or in node failure. If the damage is in the link then the cable cut may be the probable reason and on the other hand if damage is in the node, then the reason is mainly due to hardware or software faults. The impact of loss due to failure in fiber or failure in node can be analyzed by taking the log of the affected users. The number of affected users multiplied by the total time at which data transmission was not available will give the correct assessment of loss. In early days, faults were recovered manually by sending the operator for correction. Manual correction requires more time as it also depends on the skill & knowledge of the operator. Now the scenario has changed, the manual re-routing techniques is considered as unprotected for data transmission. Customers are interested in a system where very less human intervention is available and the survivability process can be done remotely reconfiguring and re-routing. For the automatic recovery different techniques are used which not only give the privilege of remote management of fault by software but also reduce time for fault correction. Using a single channel for data transmission is considered as inefficient as the rate of traffic among networks is increasing every day. So, like in wavelength routed WDM networks multiple channels are used for data communication from one place to another.[1] The Optical Ethernet is classified into three basic building blocks namely Ethernet over Fiber, Ethernet over resilient packet ring, Ethernet over dense wavelength division multiplexed networks. In this paper, section II describes about basics of Ethernet, section III provides the details about the building blocks of Optical Ethernet, section IV gives details about capabilities of Optical Ethernet and section V describes the protection and restoration techniques for Optical Ethernet network.

II. BASICS OF ETHERNET

With the increase in number of users for data communication, there is need for increasing the band width. In the traditional OSI layer, data is written in the application layer, the written data is further encoded, compressed, encrypted and decrypted in the presentation layer. In the session layer communication management is carried out. The next layer is transport layer where the data segmentation is done which is followed by network layer. In the network layer the data is put into different packets the packet is then converted into frame in data layer. Data which is available in digital form is converted into analog form in the physical layer. The signal is then passed to Ethernet, cost-effective technology which has made the data communication simple, efficient and reliable. To meet high speed requirement of data transfer, number of changes have been done in basic Ethernet LANs. In the figure the relation between the data link layer and physical layer in OSI has been depicted. The protocol stacks which are specific to Ethernet are media access control (MAC), Signaling and media. Layer 2(Data layer) and layer 1(Physical layer) functionality is enhanced by Ethernet. Media sub layer takes care of signal transmission from source to destination. Physical signaling does the documentation of the method of bit encoding and the rate at which the bit is converted. The logical link control (LLC) is used for multiplexing, error control, broadcasting, and flow control operations. The MAC layer converts the bits into frames before transmission from source to destination and error detection is also carried in this layer. The logical link sub layer and Mac bridge sub layer defined in IEEE as 802.2 and 802.1D. VLANs capabilities are covered in 802 LAN. [2]

The frame format of Ethernet is shown in figure 2. The first 64 bit is provided for preamble which gives the alert information to the destination about the start of data transfer. Next 48 bit is for MAC destination address and which is followed by 48 bit Source MAC address. 16 bit length type has been provided for data length. The total length is 1518

ISSN: 2277-3754
ISO 9001:2008 Certified
International Journal of Engineering and Innovative Technology (IJEIT)
Volume 5, Issue 4, October 2015

bytes, in which 46 to 1500 bytes is for data logical link control. The last 32 bit is allotted for check sequence. For check sequence the data is calculated in the transmitting end and forwarded to the destination. In the receiving end re-computation is done which ensures the correctness of data after transmission.

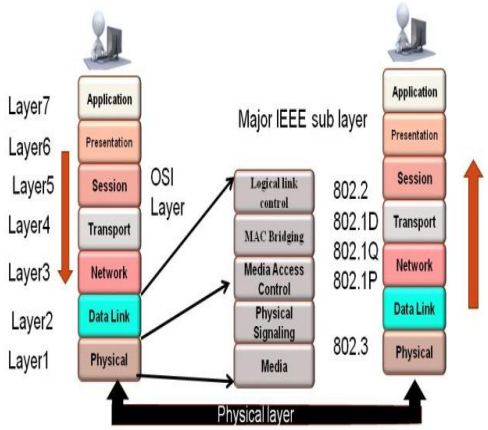


Fig 1: OSI layer and Major IEEE sub layers

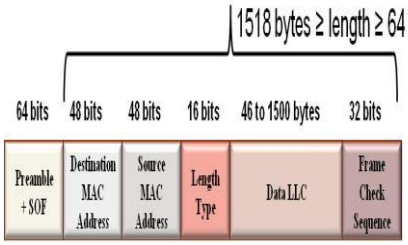


Fig: 2 Ethernet Frame format

The evolution of Ethernet started with half duplex where only one way communication was possible at a time and if communication is done through both side, then collision occurs. CSMA/CD (carrier sense multiple access with collision detection) was used widely in wired LANs to resolve the collision in the half duplex system where coaxial cables were used. Further improvement has been done by the addition of unshielded cable with repeaters and then shifted to full duplex. Later, Ethernet bridge/switch architectures which were collision free where used. Initially 10 Mbps was the speed and thick coaxial cable were used and they are called standard Ethernet. Later on a thin coaxial cable named 10 BASE2 were introduced. In 1990, 10BASE-T was introduced with unshielded twisted cable. With the use of full duplex systems with Ethernet bridge/switch architectures, collisions are avoided because it has a device to store and forward the frame and would buffer incoming frames and wait until the outgoing ports were free to transmit them. This system eliminates the requirement of CSMA/CD.

Figure 3 shows the evolution of Ethernet from half-duplex to the shared channel system using repeaters and then later in the 1990's full duplex Ethernet bridge/switch architectures, which is collision free.

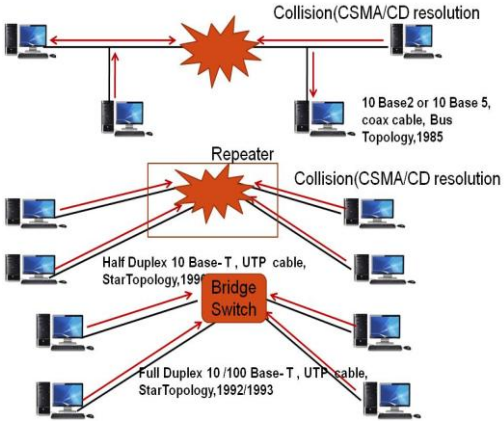


Fig 3: Ethernet basics

III. OPTICAL ETHERNET BUILDING BLOCK

The technology which delivers high-speed data communication, with storage facility, and enhanced voice and video applications is termed as Optical Ethernet. The flexibility and simplicity of Ethernet and speed and reliability of Optics is combined to enhance the data transmission capacity in optical Ethernet. Optical Ethernet building blocks are Ethernet over Fiber, Ethernet over Resilient Packet Ring (RPR) and Ethernet over Dense wavelength division multiplexing (DWDM). Point-to-Point & Mesh topology is used for data communication in Ethernet over fiber. In Ethernet over RPR uses ring topology and provides less than 50ms failover. Ring, mesh and point to point topology are used in dense wavelength division multiplexing (DWDM). [3]

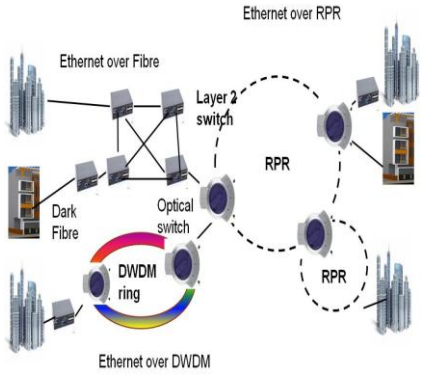


Fig 4: Building blocks of optical Ethernet [3]

IV. FEATURES OF OPTICAL ETHERNET

A. Virtual LAN (VLAN) capability

802.1Q provides the VLANs features. Nodes can be connected without any physical connection with each other using VLANS. It makes a logical link between the nodes in the same group. The Ethernet frame is composed of an additional header VLAN tag, which has a 12 bit VLAN ID and 3 bit User Priority field for virtual LAN connection. This capability helps in distributing the traffic in the network more effectively. The virtual LAN (VLAN) services are useful for enterprise networks, and thus it can be used for MAN carriers

ISSN: 2277-3754
ISO 9001:2008 Certified
International Journal of Engineering and Innovative Technology (IJEIT)
Volume 5, Issue 4, October 2015

to support in providing transparent LAN services. VLANs are important to enterprise networks because it allows them to segregate their layer 2 networks into smaller groups also making the network to be scaled for larger distances. VLANs also are useful in maintaining the traffic in the network and thus allowing more efficient load distribution.

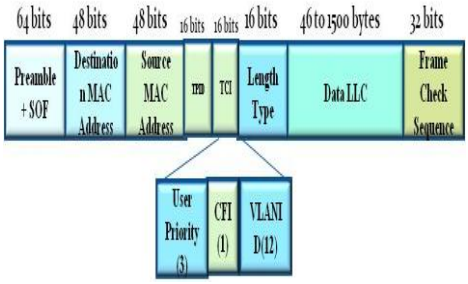


Fig 5: VLAN tag

B. Spanning tree routing

In spanning tree which is provided by 802.1D, data routing is done with the help of Spanning Tree protocol. In the event of failure the link or the node will be communicated for reconfiguring the network to new spanning tree shortest distance cost is the base for reconfiguration of the node. Rapid spanning tree is provided by 802.1w. It provides a backup port on bridge in the event of a failure Physical connectivity can be obtained within 10msec if fault is in forward state. If there is no backup, then handshaking is done with any one of the remaining active port. The spanning tree protocol also ensures the data, in the form of packet should not enter in an endless switching from one node to another. The role of different ports in the STP topology are root for selecting the best path, designated port, Alternate port is used as a backup to the root port and Backup port. Spanning tree algorithm is used for layer 2 networks. The Spanning Tree Protocol (STP) allows us to establish connection between layer 2 switches with the help of control messages so that even when a node or link failure occurs they can convey the message to each other. Spanning tree provides an alternate backup path. [4]

C. Aggregate Link Capability

Link aggregation has a group of links between switches. When fault occurs, the aggregate link capability provides a fast failover. It is a service provide by 802.3. It is used for sending and receiving traffic from one node to another. The protocol makes a virtual interface between nodes. Multiple links are regarded as one logical link to spanning tree algorithm. In the event of fault in one link fast failover of less than 1 second is done as redundant links are available. It has the provision of having multiple links between two switches which are seen as a single logical link to the spanning tree algorithm. Link aggregation is also provides services in redundant and diverse link capacity which provides faster recovery of a link failure. Also, the Gigabit Ethernet networks could be recovered faster with minimal recovery times in case of fiber cuts.

D. CoS Priority Indication

The VLAN tag are used for making logical links, has a 3-bit user priority used to identify class of service. CoS priority indication performs the traffic aggregation by queuing disciplines for allocating bandwidth and giving priority service. The packets of data go from data layer to network layer, and vice versa. Thus layer 2/3 priority handling of the packets is accomplished. All of the queuing and scheduling techniques that are used at layer 3 have also been implemented in the layer 2/3 Gigabit Ethernet switches.

V. SURVIVABILITY TECHNIQUES

Survivability is the property of a network to be resilient to failure. Protection techniques, backup nodes or links are reserved in advance for protection. Spare backup is located when the fault occurs with the help of redundant path and restoration protocol. Fault management scheme ensures the protection technique when fault is detected Fault Detection — IEEE 802.1ag support fault detection through Continuity Check messages (CCM). Messages are sent from the source to destination node at periodic intervals and if the check message is not received in both the ends within the stipulated time, then a fault are detected against the service. Fault verification - the IEEE 802.1 support fault verification. This is done through Loopback messages (LBM) and Loopback reply (LBR). The configuration is done during initial set-up or after a fault has been detected. Fault isolation - IEEE 802.1ag support fault isolation through Link trace Messages (LTM) and Link trace Reply (LTR). Fault notification - fault notification through Alarm Indication Signal (AIS). [5] Fault management can be further classified as follows.

1. *Link protection:* During the setup of any connection for data communication, backup paths are assigned for each primary link. If a failure occurs then the link will be rerouted to the reserved path. All the connections traversing the failed link and the destination and the sending station will not be affected due to this loss of link failure.

2.*Path protection:* During the setup of any connection, the source and destination backups nodes for each link are reserved, if a failure occurs then the defected path details is informed to the source and the destination nodes and reserved resources is utilized.

3. *Link Restoration scheme:* If failure occurs then the failed links participate in distributed algorithm and dynamically locate a new route. The algorithm searches the new route and when a new path is obtained then the optical interconnect establish a new connection through the new route. Connection is dropped if no new route is established.

4. *Path Restoration scheme*: If failure occurs then the failed source and destination nodes independently located a new node. The node can have different wavelength. The network elements are reconfigured and rerouted to new path. Connection is dropped if no new route is established.

5. *Sub Path Restoration scheme*: The upstream node of the failed link detects the failure and locates a backup route to the corresponding destination node. Suppose a new path is

ISSN: 2277-3754
ISO 9001:2008 Certified
International Journal of Engineering and Innovative Technology (IJEIT)
Volume 5, Issue 4, October 2015

obtained then the network elements like the optical interconnects establish a new connection through the new route. If a new route is not obtained then, the connection is dropped.

Restoration Techniques

Depending upon the type of Network different types of restoration techniques are used. The classification of restoration techniques are given below:-

A. *Reactive*- In reactive technique, alternate route is located after the fault occurs.

B. *Proactive* - In this technique alternate route is pre planned. If any failure occurs between the source and destination, signal travels from the backup path. The proactive restoration technique is further divided into different categories

1. Link based and path based- In link based scheme, reroute is done for the failure link. New completely dedicated alternate path is used for path based scheme

2. *Backup Multiplexing* - This multiplexing technique allows other backup paths to share the same wavelength. This is used for single fault check assuming only one fault in the link. If more than one fault is available, then the same wavelength and path can be shared for backup. The primary path can be used as backup for one or more demands. The primary path is in working mode, then the backup facility is inactive and when the primary path is not in working, it can be used as backup on demand.

3. *Primary Multiplexing*-A primary path may be set up on a wavelength for data transfer that is used as a backup for one or more demands.

4. *Failure-Dependent*-This is also a path-based scheme where the backup path is dependent on the particular failure may it be node failure or link failure. A backup path is made available for each possible failure on the path.

5. *Failure-Independent* schemes are used to find the link and node disjoint path and accordingly backup path provided is used. [6]

VII. SOME OF THE EXISTING PROTECTION TECHNIQUES

A. Unidirectional Path Switched Ring (UPSR)

Protection switching is handled in each direction separately in unidirectional protection. Unidirectional Path-switched Rings can handle node, link, receiver or transmitter failures easily. Signaling protocol is not needed for UPSR. In UPSR, the working bandwidth is equal to the redundant bandwidth and cannot be reused for other connections. UPSRs are popular in lower speed access networks. Fiber cuts are handled with unidirectional protection, but in the case of, transmitter failure, unidirectional protection only switches the failed direction to another path.

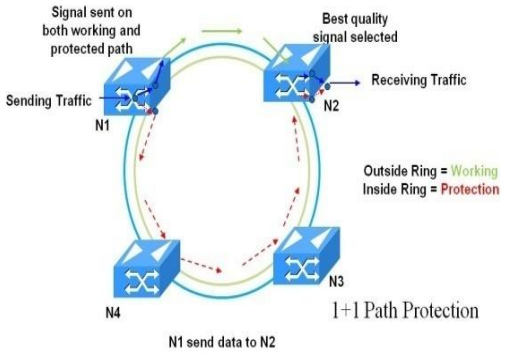


Fig 5: Unidirectional Path Switched Ring (UPSR)

In the Unidirectional Path Switched Ring, signal is send from the working node and protection path. In the communication process, two light paths are propagating in opposite direction. The best quality signal s selected in the receiver node. Figure depicts the working of UPSR wherein the working light path is from the outer ring and the protection light path is from the inner ring if a failure occurs in the working link, then the receiver node changes the protection link. If the working path between nodes N1 to node N2 fails, then message is sent from N1 to N2 after passing nodes N3 and N4 using a protection path. This protection technique is termed 1+1 protection. Due to this protection link, the restoration of failure in the node or link is much faster. [7]

B. Bidirectional Line Switched Ring (2-Fiber BLSRs)

In bidirectional protection, protection switching is handled on both directions simultaneously. BLSR is more sophisticated than ULSRs. In BLSR/4 two fibers are used as working and two fibers are used as protection. Data can be carried in both directions. BLSRs support up to 16 nodes. Span Switching Connection is rerouted on a spare link between the same nodes. In a BLSR/2, the protection fibers are "embedded" into the working fibers by sharing the bandwidth of a fiber, thus half the capacity of the fibers is reserved for protection purposes. Span switching is not possible, yet ring switching works similar to that of BLSR/4. The protection bandwidth in both BLSR cases can be used to carry low-priority traffic.

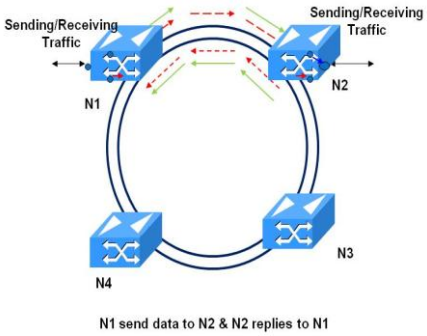


Fig 6: Bidirectional Line Switched Ring (2-Fiber BLSRs)

In bidirectional line switched ring, the signal is send from the source node to destination node. If the failure occurs in the link, the signal is looped back in the opposite direction and move to the destination node with the help of restoration

ISSN: 2277-3754
ISO 9001:2008 Certified
International Journal of Engineering and Innovative Technology (IJEIT)
Volume 5, Issue 4, October 2015

protocol. If failure occurs in node, line switching is performed in both side of the failed node.

C. Bidirectional Line Switched Ring (4-Fiber BLSRs)

In bidirectional line switched ring, 2 working link and 2 protection link is available. In the event of failure, both the transmitting node and receiving node switched over to the protection link provided. In case of no failure, the protection link can be used for transmitting the signal which has low priority traffic. During the event of failure the receiving node detects and communicates the failure to source node. The signaling protocol communicates about the failure in the link to source node and for further switch over to link provided for protection.

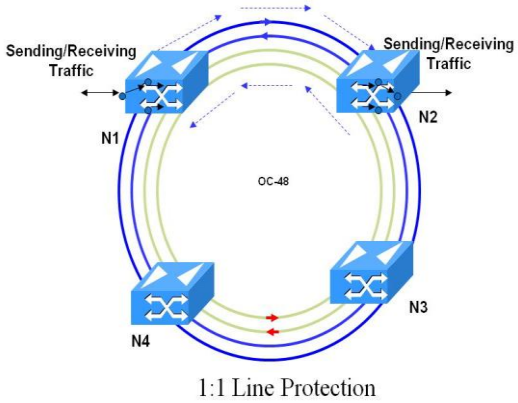


Fig 7: Bidirectional Line Switched Ring (4-Fiber BLSRs)

D. Path Protection / Line Protection

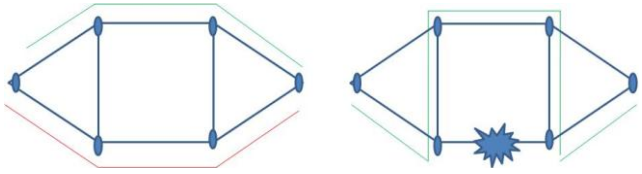


Fig 8: Path Protection / Line Protection

In line protection, a backup path is reserved at the time of primary communication setup. If any failure occurs, the restoration is handled by receiving nodes. The backup path is having the same wavelength as the primary node in the receiving end. In path protection, backup facility is reserved for primary path. Restoration is handled by both the transmitting node and the receiving node.

E. Shared Protection

In shared protection, backup facility is shared by all the links. In shared network, the working and protection link is provided. The protection is common for a group of working links. Figure 9 illustrates the working of protection technique in shared network. Switch 1 of transmitting node is connected to switch 1 of receiving node. Similarly switch 2 and 3 of transmitting node is connected to switch 2 and 3 of receiving node. Signal from transmitter is connected to one additional link through switch b of transmitting node and switch b of receiving node to original node. Switch. If any failure occurs, the signal is diverted from the working path to protection path.

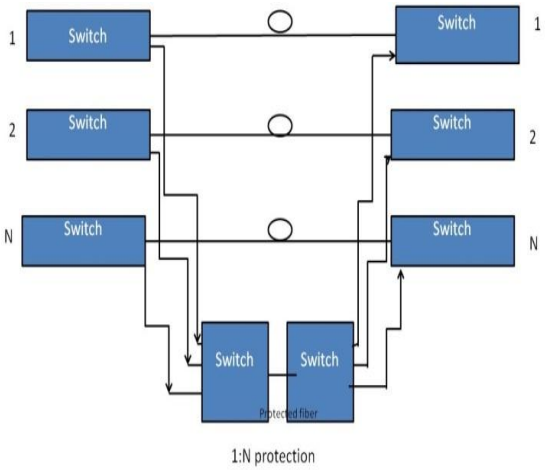


Fig 9: Shared Protection

F. Fast-Protection in Ethernet Over Resilient Packet Ring (EoRPR): Using Wrap

The IEEE 802.17 Resilient Packet Ring (RPR) is standardized by IEEE, new scheme for Metro Ethernet domain. It is an Ethernet based scheme with efficient bandwidth suitable for multicast traffic. Complex signaling mechanisms is incorporated in RPR for fairness of bandwidth sharing between the ring nodes. It is a difficult protocol to implement efficiently and correctly. [7]

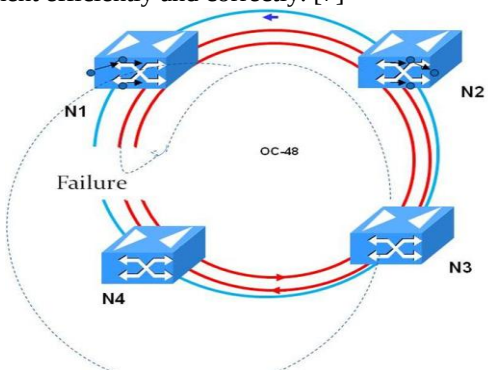


Fig 10: Protection in Ethernet over Resilient Packet Ring (EoRPR): [8]

Data is sending in packets in Ethernet over resilience packet ring. Signal is send from node to another, the node further forward the signal to next node in the ring. If a fault is occurs in the in the path, then through wrap or steering method protection is done [8].Figure illustrates the working of protection in EoRPR. N3 node is transmitting signal and signal is propagating through N4 to the destination N1. If failure occurs between N4 and N1, then signal will wrap through the inside ring and reach the destination node N1. The path traveled is non-optimal, but as this has a fast healing property, it automatically selects the optimal path. In steering method, the packet ring protocol is used to reroute the path in the event of failure. In steering or wrap method, the signal is diverted to another route and the failover is less than 50m second.

ISSN: 2277-3754
ISO 9001:2008 Certified
International Journal of Engineering and Innovative Technology (IJEIT)
Volume 5, Issue 4, October 2015

G. Ethernet passive optical network (EPON)

A new emerged network system, called Ethernet passive optical network uses Ethernet and fiber for transmission of traffic from one place to other. It is point to multipoint optical communication technology. There is no active elements used in the signal path from source to destination for transmission, optical splitters and optical fibers are the only passive components used. The architecture of Ethernet passive optical network comprises of optical line terminal and multiple optical network unit. In the central office, the optical line terminals are available which connects the signal to the destination and the access may be in MAN or WAN system. The optical network units are available to subscriber under fiber to the home architecture, fiber to Business architecture or as fiber to the curb architecture.[9] The figure 11 shows the working of point to multipoint system where single fiber coming from the output network terminal (OLT) is connected to 1: N optical splitter. The splitter is connected to different network units. The traffic is traveling from the optical terminal unit (ONU) to optical network unit in downstream point to multipoint communication system and signal moves from optical network unit to optical line terminal in upstream multipoint to point communication system. EPON uses two wavelengths for upstream and downstream transmission. For transmission of signal multipoint control protocol is used. It is a signal access protocol and is standardized by IEEE 802.3ah. For assigning bandwidth to different optical network units, dynamic bandwidth allocation algorithm is deployed in optical line terminal.

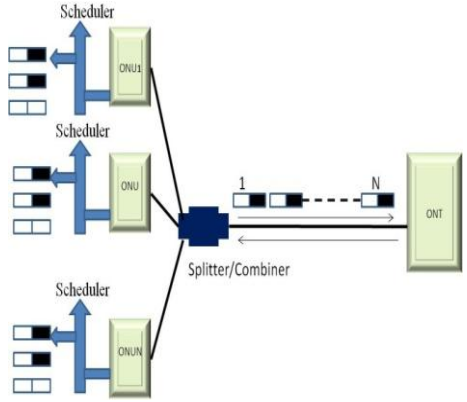


Fig: 11 Ethernet passive optical network architecture

The common failure in Ethernet passive optical network are fiber cut in feeder or drop fiber, failure in Optical Line Terminal and Optical Network Unit transceiver and failure in the optical components such as passive splitter and combiner, connectors and splices etc. fault localization and detection in EPON can be done by fiber plant monitoring by OTDR. Transceiver status monitoring provides the network operator to monitor major optical transceiver parameters for both Optical Line Terminal and Optical Network Units. Optical Network Units connect to the Optical Line Terminal through two different routes to form two PON links. Each link is a backup to the other. In normal conditions, two Passive Optical Networks carry services at the same time. When one optical network Unit or a Passive Optical Network link of several Optical Network Units fails because of fiber or optical transceiver failures, this Optical Network Unit or these Optical Network Units will transfer all their services to the other available Passive Optical Network link. Switches are performed according the services' priorities: first transmit high priority services to ensure the quality of service (QoS) requirements [10]

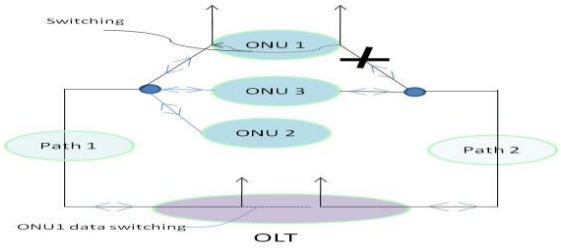


Fig: 12 illustrating the protection in Ethernet passive optical network.

H. Protection in Ethernet over Dense Wavelength Division Multiplexing (DWDM)

Point-to-point topology is used for long-haul transport having ultrahigh speed, reliability, high signal integrity, high bandwidth in terabits per second and fast path restoration capability. The long distance coverage between transmitter and receiver is effective done with the help of the number of amplifiers between the two end points. Drop and add channels in the path of Point-to-point communication system is accomplished by add-drop multiplexing. The parameters used in the calculation of the power budget are channel spacing, type of fiber, signal modulation method and number of channels. In DWDM, each channel is carried over optical channel. Different channels may carry different data at different bit rates. The optical link of transmitter-receiver has several optical components such as fiber(s), OADM, optical amplifiers, couplers, laser sources, optical filters, and modulators and receivers.

1. Point-to-point topologies and its protection

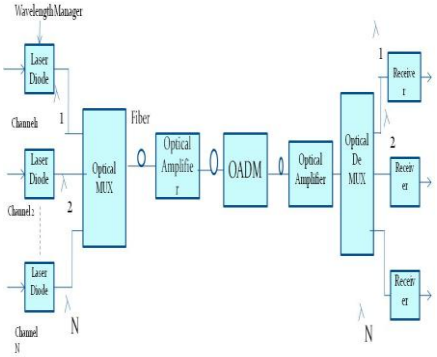


Fig 13: Point-to-point topologies and its protection [11]

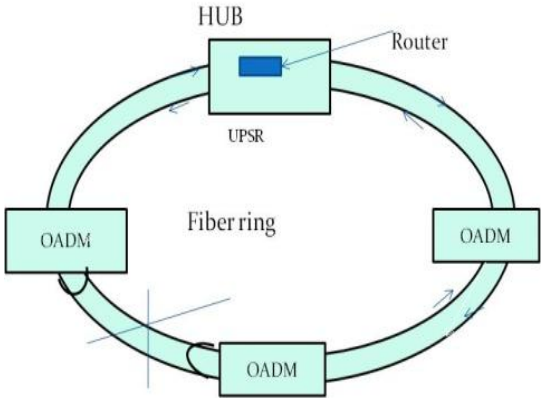
In the point to point topologies, the signal coming from the different channel is fed to laser diode where the signal is converted into different colors of light having different wavelength. The light is then travels through the multiplexer to optical amplifier. The signal strength reduces after passing through multiplexer and before the entering the signal in de-

ISSN: 2277-3754
ISO 9001:2008 Certified
International Journal of Engineering and Innovative Technology (IJEIT)
Volume 5, Issue 4, October 2015

multiplexer. to enhance the same optical Ethernet is used. The amplified signal is then given optical add drop multiplexer (OADM). OADM is used to add or drop the channels. The signal then passes through the de-multiplexer to respective receiver. If a fault occurs in the fiber, the signal is routed through the alternate path.[11]

2. Ring Topology and its protection

DWDM networks must be able to isolate a fault or to detect faults on the link. The objective is to offer continuous transmission or service with the minimum disruption possible, as recommended in the standards. Depending on network topology and design, fault avoidance may be accomplished with dual counter rotating rings. When a fault is detected in a counter rotating ring design, the neighboring OADMs avoid the fault by rerouting traffic via a U-turn optical cross-connect. In point-to-point topology, detected faults will trigger a approach that either finds an alternative path or causes alarms. In mesh architecture, faults will trigger a different path selection approach that bypasses the fault. Fault avoidance requires complex optical cross connect devices that increases cost budget and burden on the power of the ring network.



In the ring topology, signal coming from different channel is managed by hub. The OADM can drop or add the channel. If the signal traveling in the channel is blocked due to fiber cut, the OADM near to the fault will reroute the signal through a U turn cross connect and signal is received by the destination from a different path. When the fault is restored, the ring network will return in the normal path. [12]

VIII. CONCLUSION AND FUTUTRE SCOPE

Optical Ethernet represents one of the most interesting solutions for high-speed and reliable data communication. Impact of data loss is huge that is way different types of protection techniques have been adopted to overcome the problem of failure. In this paper the existing protection techniques for Optical Ethernet over fiber, over resilience packet ring and over dense wavelength division multiplexing were presented. The resilience packet ring uses steering or wraps method for re-routing and selecting optimal path for data transmission automatically after the failure. The DWDM gives better bandwidth coverage. The incorporation of device such as multiplexer and OADM have made the re- routing technique more efficient and intelligent. As customer needs reliable and protected data transmission with fast restoration, the work has to be more done in DWDM technology for more efficient protocol and fast restoration technique.

REFERENCES

[1] Guido Maier, Achille Pattavina, Simone De Patre, Mario Martinelli, Corecom, "Optical network survivability: protection techniques in WDM layer", Photonic Network communication, Kluwer Academic Publishers.

[2] OSI model - Wikipedia, http://en.wikipedia.org/wiki/OSI_model

[3] Optical Ethernet Overview, white paper, Nortel Networks.

[4] Spanning tree algorithm, Wikipedia, http://en.wikipedia.org/wiki/spanning tree.

[5] "Ethernet as a Carrier Grade Technology: Developments and Innovations", Hellas-On-Line, Corporate Services Division.

[6] Osameh M. Al-Kofahi, Ahmed E. Kamal, Department of Electrical and Computer Engineering, Iowa State University, "Survivability strategies in multihop wireless networks "

[7] Himanshi Saini, Amit Kumar Garg, "Protection and Restoration Schemes in Optical Networks: A Comprehensive Survey", International Journal Microwaves appl.

[8] Srivas Chennu, Kai Habel, Klaus-Dieter Langer Fraunhofer Institute for Telecommunications, "Protected Ethernet Rings for Optical Access Networks", Berlin, Germany

[9] "An Introduction to Resilient Packet Ring Technology", A White Paper by the Resilient Packet Ring Alliance October 2001.

[10] "EPON Technology", White Paper GW technologist Co., Ltd. Shangdi Xilu, Haidian District, Beijing.

[11] Introduction to DWDM Technology, CISCO Systems, Corporate Headquarters, Cisco Systems, Inc. 170 West Tasman Drive, San Jose, CA 95134-706,USA,http://www.cisco.com

[12] DWDM Topology, tp.utcluj.ro/pub/users/cemil/dwdm/dwdm_Intro/ 16_5311757.pd.