The Dedicated Optical Connection Protection with IP Traffic in WDM Mesh Networks

Stefanos Mylonakis, Member IEEE

***Abstract*-The optical networks based on WDM (Wavelength Division Multiplex) technology can carry enormous amount of data in each fiber link in the network. The networks with the high capacity links have the drawback that a single failure leads to the loss of a large amount of data. So a protection strategic is critical to protect from faults both service providers and end-users. IP networks carry many types of traffic. Such traffic is web, email, voice, audio and video. In this paper the problem of traffic IP over WDM mesh networks is studied when each IP connection is protected by dedicated optical connection protection. It is also the network performance is presented.**

Key words: dedicated protection, IP traffic, loss, performance

I.INTRODUCTION

The optical networks based on WDM technology can carry enormous amount of data in each fiber link in the network. But the popularity of the Internet is promising enormous growth in data traffic originating from hosts that are IP endpoints. This growth is being fueled by various applications such as those of World Wide Web (WWW). The multiparty networked applications are gaining interest in areas as online games, e-learning, e-health, and collaborative work depended on a set of common functions. Next generation networks also offer new opportunities and challenges to Internet service providers as well as providers of other line services. Research has been done in relation to the methods and the problems associated with planning, protection and restoration of optical networks with IP traffic. In [1], there are issues of modeling and analysis. In [2], there are software issues. In [3], there are issues of computer communication networks. The network survivability has been extensively studied. There are several approaches to ensure fiber network survivability [4], [5].In [6] the authors present a simple integrated provisioning / protection scheme to dynamically allocate restorable bandwidth guaranteed paths in IP over WDM networks. A guaranteed restorable path implies that a flow of data is successfully routed if both an active path and another alternate link disjoint path are found at the same time. In the [7], [8] addresses issues in designing a survivable optical layer. In [9], the approach of path protection is examined, its wavelength capacity requirements, the routing and wavelength assignment of the primary and backup paths, as well as the protection switching time and the susceptibility of these schemes to failures. In [10], the bursty nature of IP traffic is showed and its impact on WDM networks. In [11], it is proposed an analytical model for the access and core network nodes of multi-service mesh network architecture which operates in a synchronous slotted transmission mode and in [12] the author deals with the modeling and simulation and gives practical advices for network designers and developers. In [13] the authors deal with a new Service Traffic Management System.

Manuscript received April 5, 2012. St.T. Mylonakis is with the National University of Athens, Athens, Attica, GREECE (corresponding author to provide phone: 00302108814002; fax: 00302108233405; e-mail: smylo@ otenet.gr).

The objective is to solve the dedicated protection connection problem and to present the results of the performance of the network when the traffic is IP. The network is an optical WDM mesh network (core network) which carries IP packets directly over the optical layer [3]-[13]. At any time , there are two default (preplanned) diverse lightpaths through the WDM mesh network connecting two hosts, one for working and one for protection. The performance of the system is dependent on the maximum number of requests for connection that network can carry and the WDM system capacity. The network topology and other parameters are known as WDM and optical fiber capacity, one optical fiber per link with an extension to a 1+1 fiber protection system with nodes having wavelength conversion capability. So this network is characterized by one working fiber per link, edges of two links, links of two optical fibers, one for working and one for protection. The connections are lightpaths that originating in the source nodes and terminating at the destination nodes proceeding from preplanned optical working paths. Additionally, the same number of optical paths are preselected for the preplanned fully disjoint backup paths, (1+1 dedicated protection connection). Thus the connections that have been set up are protected. The number of the connections of each node pair is produced randomly but its maximum value could be adjusted properly. So the connection group size of each node pair is variable. The IP traffic is generated randomly for each user and arrives to the source node by access network. The connections of the same node pair by same preplanned optical paths form a connection group along the network. The dedicated protection of the connection groups is done by preplanned optical protection paths with the use of a suitable number of wavelengths per link along the network. The problem solution is to calculate the network performance.

This paper is broken down in the following sections: Section II describes the problem and provides a solution, the synoptic method description, its example, the proposals and a discussion; Section III draws conclusions and finally ends with the references.

II.THE PROBLEM AND ITS SOLUTION

A. The problem

The network topology and other parameters are known as WDM and optical fiber capacity, one optical fiber per link with an extension to a 1+1 fiber protection system with nodes having wavelength conversion capability. So this network is characterized by one working fiber per link, edges of two links, links of two optical fibers, one for working and one for protection. The connections are lightpaths that originating in the source nodes and terminating at the destination nodes proceeding from preplanned optical working and protection paths. The IP traffic is generated randomly for each user and arrives to the source node. The connections of the same node pair by same preplanned optical paths form a connection group along the network. The problem solution is to calculate, first and second, the network performance.

TABLE 1
THE SYMBOLS OF THIS PAPER

S/N	Symbol	Comments
1	q	The node number
2	p	The edge number
3	G(V,E)	The network graph
4	V(G)	The network node set
5	E(G)	The network edge set
6	2p	The number of working and backup fiber for 1+1 line protection
7	n	The number of source – destination nodes pairs of the network
8	ρ	Average connection utilization (ρ)
9	Ts	Average packet serviced time (Ts)
10	*T*a	Average packet arrival time (Ta)
11	k	Average packet length (k)
12	R_b	line bit rate
13	n(i)	The number of the connection groups that passes through the fiber (i) and means that each fiber has different number of connection groups pass through it.
14	$n(i)_w$	The number of the working connection groups that passes through the fiber (i).
15	$n(i)_{pr}$	The number of the protection connection groups that passes through the fiber (i).
16	$\Delta y_{w\,i,j}$	It corresponds to group of working optical connections that passes through the optical link (i) with number (j).
17	$\Delta y_{pr\,i,j}$	It corresponds to group of protection optical connections that passes through the optical link (i) with number (j).
18	K	The number of the wavelengths channels on each fiber that is the WDM system capacity
19	$C(i)_b$	The busy capacity of each fiber link (i)
20	Cinst	The total network installed capacity
21	Tro	The offered traffic
22	Trs	The serviced traffic
23	Trl	The loss traffic

B. The formulation

The IP packets are aggregated and forwarded to the input nodes of the mesh network and requested for connection to be transported at their destination [3], [10] and [11]. But in some time periods, the number of requests for connection of each node pair is larger than that could be carried by the optical network. So IP traffic could be blocked and cleared. At the input nodes, the packets are forwarded to their destinations according their optical working paths and optical protection paths using different wavelengths at each link because the network has wavelength conversion. Each connection can modeled as an M/G/1 system (buffer size equal to zero) that is, a connection of two optical preplanned paths one for working and one for protection ,1+1 optical path protection , which operates as one pipeline that passes packets with Poisson packet arrival times . The assumption of Poisson arrivals, for the input flows is accurate if the observation interval is not large (short-range dependent). This happens since the aggregate traffic in each connection consists of many small and independent arrival processes that corresponding to the traffic generated by a single user, as the number of independent arrival processes of the single user increases, the aggregate traffic asymptotically tends to follow Poisson statistics.

The following parameters are interesting for the network performance.

Total offered user number and *Total serviced user number* means the total number of the users that required for connection and serviced respectively.

Total offered packet arrivals number and *Total serviced packet arrivals number* means the total number of packets that are generated by users, arrived at the input (source) nodes of the optical network and serviced respectively.

Average serviced packet arrivals per user means the average of the packets that corresponded to each user and serviced by the optical network.

Total packet length means the total length of the packets that serviced by optical network.

Average packet length per user means the average length of the packets that corresponded to users that serviced by optical network.

Average packet arrival time means the average of the arrival time of the serviced packets and equals with one second.

The average connection utilization is dependent of the average arrival rate and means service time. *Average connection utilization* (ρ) is provided by the ratio of *Average packet serviced time* (Ts) with *Average packet arrival time (Ta)*.

$$\rho = Ts/Ta \tag{1}$$

Average packet serviced time (Ts) equals with the ratio of the average packet length (k) to line bit rate (R_b),

$$Ts = k / R_b \tag{2}$$

The total busy capacity $C(i)_b$ of each fiber link (*i*) is given

$$C(i)_b = \sum_{j=1}^{n(i)_w} \Delta y_{w\,i,j} + \sum_{j=1}^{n(i)_{pr}} \Delta y_{pr\,i,j} \tag{3}$$

with $n(i)=n(i)_w + n(i)_{pr}$, the total number of connections that pass through this link. $\Delta y_{w\,i,j}$, $\Delta y_{pr\,i,j}$ correspond to group of working and protection optical connections that pass through the optical link (i) with number (j).

C. Synoptic description of the method

The method describes the operation of the WDM optical fiber mesh network with 1+1 optical fiber protection, the working connections passed through preplanned optical paths but when a failure occurs the traffic is passed through preplanned protection paths. It has two parts, the first part or the planning and designing phase and the second part or network with failure phase. So when a cut occurs, the network has failure and the preplanned protection method is activated. The network has links with a finite, nonzero capacity and the link capacity is not exceeded. This method is driven by suitable data and then simulates the actual dynamic behavior of the network. Simulation language is critical to the economic feasibility of this entire investigation. TURBO PASCAL is

used to program the model [1], [2] and [12]. The IP users send at the input nodes of the WDM network, a large number of small size packets. The packets of each IP user are aggregated to larger packets and forward to their destinations using a protected connection. The number of the IP users of each node pair is adjusted so that all offered traffic is not serviced or done for a time period of one second, so there is or not any loss (in this case the connection group size is also not equal or really equal with the user number). Each request for connection (offered) checks the links capacity for its capability to be done with 1+1 optical path protection according to the preplanned optical paths to be serviced or to be rejected. If a request for connection is rejected, the corresponded IP user is also rejected. Each checked working connection that could be done (the packets could be carried and serviced) , starts from the source node and progresses through the network occupying a wavelength on each optical fiber and switch to another fiber on the same or other wavelength by OXC, according to its preplanned working optical path up to arrive at the destination node. Simultaneously, the protection connection starts from the source node and progresses through the network checking to be serviced or to be rejected occupying a wavelength on each optical fiber and switch to another fiber on the same or other wavelength by OXC, according to its preplanned protection optical path up to arrive at the destination node. So there is full and dedicated protection for this connection. The number of connections of each node pair is equal to its connection group size. After a connection (working as well as protection) has been established, the available capacity is also calculated. When all connections are done the results are calculated.

TABLE 2
THE SYNOPTIC PRESENTATION OF THE METHODS

FIRST PART(*Planning and designing Phase*)
First step, network parameters reading
(q, p, V(G), E(G), G(V,E), 2,2p, k)
Second step, connection selections
(n, (S_n,D_n), Xn, Preplanned working and protection lightpaths)
Third step, checking and wavelength allocation
(Routing and wavelength assignment method)
Forth step, results
(Tro,Trs,Trl,Cav,Cb,Cinst)
SECOND PART(*Network with failure Phase)*
Fifth step. Network parameter modifications
(cut link, q, p, V(G'), E'(G'), G'(V,E'), 2,2p-1, k)
Sixth step. Traffic passing from protection path
(Dedication protection method)
Seventh step. New Results
(Tro,Tr's,Tr'l,C'av,C'b,Ci'nst)

The algorithm permits to investigate the impact of the random arrival requests for connection at the input nodes to the network capacity. The performance measurement is to count the factors that impact on the network and their relationships. The random numbers which are generated in this paper is based on the Pascal command *random(x)*.

The complexity of this method for the node number q depends on the square of the node number and the total number of the requests for connection (s) so it is written as O ($s*q^2$). The time complexity of that algorithm is 'order q^2, O($s*q^2$). Thus, on a 133MHz computer, q=6 and s=12, the time is 4 hundredths of second. It means that worst time consuming depends by the network size for the same computer. The symbols with tone mean modifications.

The synoptic description of the method is shown in the table 2.

D. Example

The network is assumed to be an optical mesh core network with the packet switched (packets switched according to preplanned paths) as a graph. Each vertex represents the central telecommunications office (CO) with the OXC while each edge represents two opposite links. Each link has a couple of optical fibers. All optical fibers have the same capacity as the WDM system. All nodes are identical. The number of working and protection connections that pass through each optical fiber is different. The topology of the network is presented by the graph G(V,E). This mesh topology is used because it is a simple, palpable and it is easy to expand to any mesh topology. The vertex set has q=6 elements which are V= {v_1, v_2, v_3, v_4, v_5, v_6} and the edge set has p=9 elements which are E= {e_1, e_2, e_3, e_4, e_5, e_6, e_7, e_8, e_9}. At the source nodes, the IP packets are aggregated and requested for connection to be transported at their destination. The number of the IP users and the corresponded number of the requests for connection are random with variable maximum value. Each IP user sends a random number of packets that are in the range of 25 and 150. The length of each packet is constant equal to eighty (80) bits. The connections of each node pair form connection groups according to its preplanned path and transverse the network. Figure 1 presents the mesh topology.

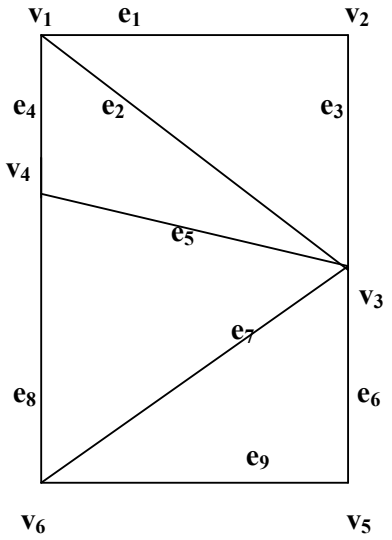

Figure1.The mesh topology of the network

The problem is solved for *an n=12 of 30 possible* node pairs. These have their order for each source-destination node pair, their working paths and their protection paths as shown in table 4. The total length of the working lightpaths is 20 and the

total length of the protection paths 27. It is also obvious that the dedicated path protection mechanisms use more than 100% redundant capacity because their lengths are longer than their working paths, protection ratio equal to 1.35. Similarly for the same connection group size the capacity that is used by the protection paths is larger than the corresponding working paths. Table 3 presents the network parameters. Table 4 present the node pairs with the preplanned working and protection paths. Table 5 presents the numbering and the connection groups of each fibre without network failure. This problem is studied for two cases.

In the first *case*, the performance estimation is investigated and represented. If the offered traffic to a link is less or equal than its capacity then it is serviced and the busy wavelengths are given by equation 3. When the offered traffic is greater than its capacity, only the traffic equal to its capacity is serviced but the redundant is rejected. The n(i) takes the values up to the link capacity is full. If a request for connection has successful working lightpath but no successful protection path, it is rejected. Each IP user sends a random number of packets that are in the range of 25 and 150 with length constant equal to eighty (80) bits and makes one request for connection. The maximum number of the IP users of each node pair requested a connection, is adjusted up to twelve (12) for a time period of one second, so there are loss and all offered traffic is not serviced by network because some requests for connection rejected. The measurement time period is ten seconds and on this time period the performance is measured. Table 6 presents the performance measurements.

TABLE 3
THE NETWORK PARAMETERS

S/N	Network parameters	Amount
1	Node number	6
2	Edge number	9
3	Working fiber per edge	2
4	Working fiber per link	1
5	Network working fiber	18
6	Protection fiber per edge	2
7	Protection fiber per link	1
8	Network protection fiber	18
9	WDM system capacity	30

TABLE 4
THE NODE PAIRS WITH PREPLANNED WORKING AMD PROTECTION PATHS

Node pair [Si,Di]	Node pair [v_i, v_j]	Working Path	Protection Path
[S_1, D_1]	**[v_1, v_2]**	**v_1, v_2**	**v_1, v_3 ,v_2**
[S_2, D_2]	**[v_1, v_3]**	**v_1 ,v_3**	**v_1, v_2 ,v_3**
[S_3, D_3]	**[v_1, v_5]**	**v_1, v_3 ,v_5**	**v_1, v_4 , v_6,v_5**
[S_4, D_4]	**[v_2, v_3]**	**v_2, v_3**	**v_2, v_1 ,v_3**
[S_5, D_5]	**[v_2, v_4]**	**v_2, v_1 ,v_4**	**v_2, v_3 ,v_4**
[S_6, D_6]	**[v_2, v_5]**	**V_2, v_3,v_5**	**V_2, v_1, v_4 ,v_6,v_5**
[S_7, D_7]	**[v_3, v_4]**	**v_3, v_4**	**v_3, v_6 ,v_4**
[S_8, D_8]	**[v_3, v_6]**	**v_3 ,v_6**	**v_3 ,v_5 ,v_6**
[S_9, D_9]	**[v_4, v_1]**	**v_4 ,v_3,v_1**	**v_4 ,v_1**
[S_{10}, D_{10}]	**[v_4, v_5]**	**V_4, v_6 ,v_5**	**V_4, v_3,v_5**
[S_{11}, D_{11}]	**[v_5, v_4]**	**v_5, v_3 ,v_4**	**v_5, v_6 ,v_4**
[S_{12}, D_{12}]	**[v_6, v_1]**	**V_6, v_3 ,v_4,v_1**	**V_6, v_4 ,v_3,v_1**

TABLE 5
THE NUMBERING AND THE CONNECTION GROUPS OF EACH FIBER WITHOUT NETWORK FAILURE

Fiber,i	Optical fiber link	n(i)
1	<v_1, v_2>	2
2	<v_2, v_1>	3
3	<v_1, v_3>	4
4	<v_3, v_1>	2
5	<v_2, v_3>	4
6	<v_3, v_2>	1
7	<v_1, v_4>	3
8	<v_4, v_1>	2
9	<v_3, v_4>	4
10	<v_4, v_3 >	3
11	<v_3, v_5>	4
12	<v_5, v_3>	1
13	<v_3, v_6>	2
14	<v_6, v_3>	1
15	<v_4, v_6>	3
16	<v_6, v_4 >	3
17	<v_5, v_6>	2
18	<v_6, v_5>	3

TABLE 6
THE PERFORMANCE MEASUREMENTS

Sec	Tro	Trl	Trs	Cb	Cav
1	73	0	73	267	273
2	70	1	69	277	263
3	80	0	80	315	225
4	66	3	63	263	277
5	87	5	82	333	207
6	87	1	86	322	218
7	96	8	88	329	211
8	81	5	76	286	254
9	93	14	79	302	238
10	73	1	72	265	275

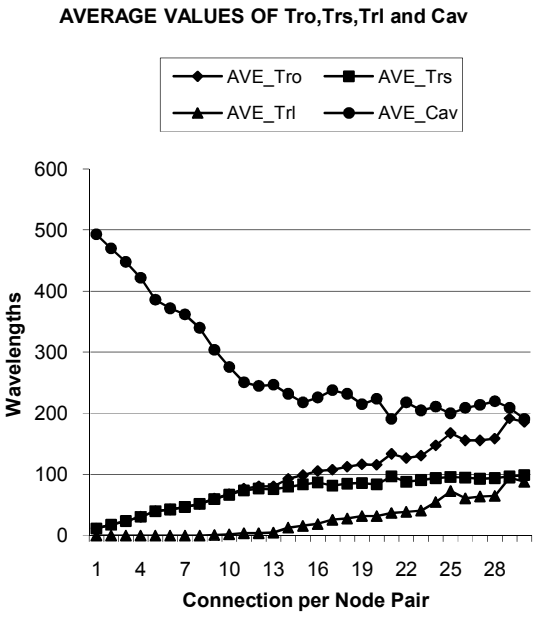

Figure2.The average values of Tro, Trs and Trl as well as Cav

It shows for the maximum number of the users and the corresponded number of the requests for connection adjusted up to twelve (12), the offered traffic, the loss, the serviced traffic, the busy capacity and the unused available capacity for each observation and for all node pairs. The average offered traffic is about 81 users per second. The standard deviation is 10. The same for the serviced traffic is 77 and 8 respectively. Figure 2 shows the average roundup values of the offered, serviced and loss traffic as well as the network available capacity when the maximum number of the IP users of each node pair requested a connection, is adjusted from one up to thirty (30) for a time period of ten seconds.

The table 7 is taken when the time interval (Ti) is broadened from T_1=10sec at T_2=100sec and T_3=1000sec. Figure 3 shows the average connection utilization Ts for minimum packet lengths equal to 2000(=25*80) bits and maximum packet length equal to 12000(=150*80) bits, for several bit rates (Rb) from low values up to high values for previous time intervals. The bit rate has been chosen so that the averaged serviced time is smaller than arrival time, ts<ta. It is assumed that the average packet arrival time is one (1) sec so the average packet serviced time equals to average connection utilization. It is also kept the average packet length constant because the parameters of table 7 are also constant so when the line bit rate increases then average connection utilization is reduced. When the bit rate is too high 1Gbps and 10Gbps its values are too small. The burstiness [10] depends of the constant average packet length and the line bit rate per wavelength so the burstiness equals to average connection utilization. The probability to transmit the symbol one (1) is given by the relationship 0.5*burstiness and the symbol zero 1-0.5*burstiness. So for high bit rates the too small value of burstiness gives too small value to transmit one. Generally adjusting all previous parameters the desired burstiness and desired probability to transmit the symbol one (1) are succeeded.

In the table 8 the limits of average connection utilization for min and max packet lengths and for several line bit rates are showed. These values are the same with those of figure 3.

In the *second case*, for the protected 1+1 connections, the main and the backup ones are led by same average packet length so their average connection utilization is the same. It is assumed than each node pair has one protected connection. So for time intervals of 10 seconds, for each 1+1 connection, the average packet length is variable. The total offered and serviced traffic is 12*10=120 connections. The bit rate has been chosen so that the averaged serviced time is smaller than arrival time, $t_s<t_a$. All times are seconds.

TABLE 7
THE PARAMETERS OF THE TIME INTERVALS 10, 100, 1000 SEC.

Description \ Time interval	T1	T2	T3
	(10sec)	(100sec)	(1000sec)
Total offered user number	806	7775	77563
Total serviced user number	768	7365	73572
Total offered packet arrivals Number	63585	616377	6132921
Total serviced packet arrivals Number	59324	581987	5819849
Average serviced packet Arrivals per user	77.24	79.02	79.10
Total serviced packet Length(bits)	47 45920	46558960	465587920
Average packet length per user (bits)	6179	6321.65	6328.30

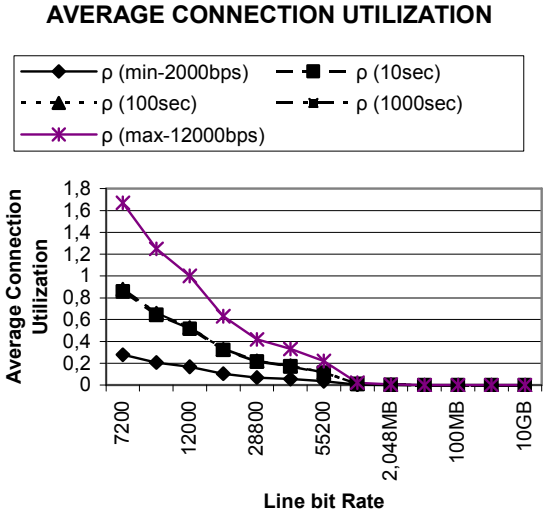

Figure 3 shows the average connection utilization for min and max packet lengths, several bit rates and 3 time intervals.

TABLE 8
THE LIMITS OF AVERAGE CONNECTION UTILIZATION FOR MIN AND MAX PACKET LENGTHS AND FOR SEVERAL LINE BIT RATES

Rb(bps)	ρ(min-2000bps) sec	ρ(max-12000bps) sec
7200	0,278	1,67
9600	0,208	1,25
12000	0,167	1
19200	0,104	0,63
28800	0,069	0,42
36000	0,056	0,33
55200	0,036	0,22
512KB	0,0039	0,023
2,048MB	0,00098	0,0059
10MB	0,0002	0,0012
100MB	0,00002	0,00012
1GB	0,000002	0,000012
10GB	0,0000002	0,0000012

In figure 4 the average connection utilization for each connection is showed and several line bit rates for time interval of 10 seconds of 120 users.

When a node pair has more than one and less or equal to seven connections, each of them has different average packet length so different average connection utilization. For the minimum and the maximum packet length, the results are the same as the table 8 respectively. For bit rate equal to 9600 bps and the time interval of 10 seconds, for each used wavelength of each fiber of WDM mesh network, the average connection utilization is showed in the followed figure 5.

E. Discussion and Proposals

Today installation of WDM networks is based on mesh topologies but the latter are essentially formed by a set of point-to-point links between nodes. Network survivability is an inherent part of the mesh topology because there are usually at least two paths between end nodes. Thus, a network that uses a

mesh topology can survive after a single failure. In communications, network survivability defined as the capability of a communication network to resist any link or node interruption or disturbance of service, particularly by warfare, fire, earthquake, harmful radiation or other physical or natural catastrophes.

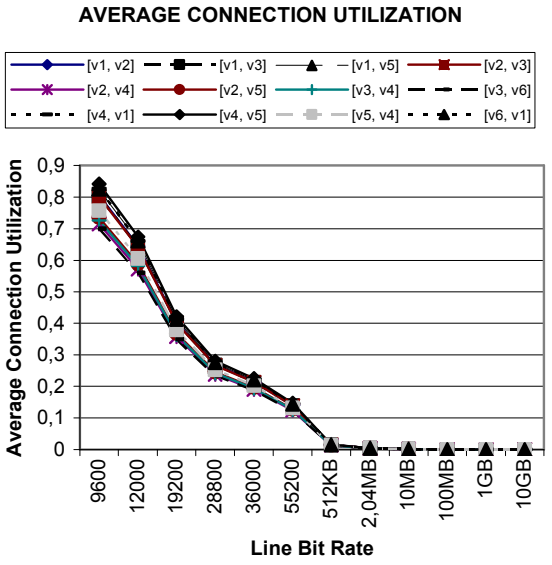

Figure 4.The average connection utilization for several bit rates for one connection for each node pair.

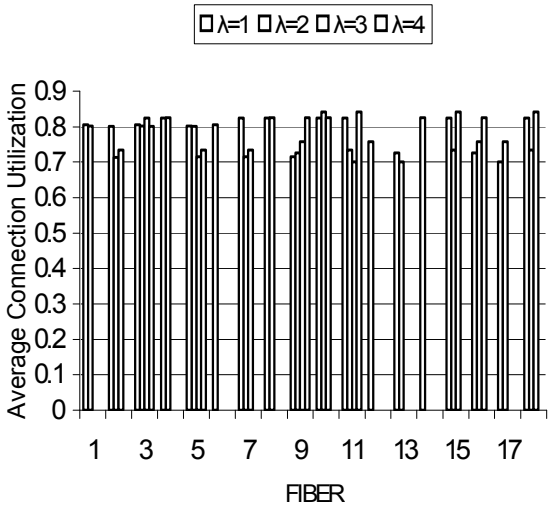

Figure 5 shows the average connection utilization for each fiber and for each busy wavelength of this fiber.

In this protection scheme, each connection of each source destination node pair is routed on the primary path and a single fully disjoint backup path is preselected for each primary path. When a single failure of a cut link occurs and the main connection also cut then the connection is routed by backup path. So this procedure is not understood by user.

For a better presentation of this research an example is used. The connection length depends on the number of hops. It is a switch packet network but the packets travel from preplanned paths so that one lightpath corresponds to one optical connection. Different wavelengths may be used for different connections in each hop, so that wavelength conversion is used at each node. When the maximum possible number of the offered traffic for each node pair increases then any link capacity is inadequate and there is loss. The network protects its connections from single link cut and any failure or failures in their paths. Initially, the performance is studied and the maximum number of the users of each node pair is adjusted up to twelve (12) for a time period of one second , so there are loss and all offered traffic is not serviced by the network. After the connection group size per node pair is adjusted successively to take values up to 30 for a time period of 10 second and the average values of the offered, serviced, loss traffic respectively as well as the available capacity are calculated. The performance is also showed for time intervals of 10, 100 and 1000 seconds with the user number to be generated randomly for each node pair of each second. It is remarkable the too small average connection utilization for high bit rates. The bit rates were selected to show the gradual passage from low values to higher ones. It explains the bursty nature of modern optical IP networks and various technologies have developed. At the end, the performance is studied for a time interval of ten seconds, the user number and the corresponded connection number is constant and equal to one for this time period as well as the line bit rate and none request for connection is rejected.

The measurement of the traffic is very important because it is essential to measure the traffic of individual services and to estimate their cost for cost accounting between service providers and ISP (Internet Service Providers) [13]. The current traffic measurements techniques only provide the total traffic volume in links, without reporting the operator whose services flow through the links. So the suitable monitoring systems should be installed in order to observe which service traffic flows in every link and can analyze the traffic of individual services based on user log data. The monitoring system can report not only the traffic of individual services in every link, but also user behavior for each service.

III. CONCLUSIONS

The optical networks based on WDM technology can carry enormous amount of data in each fiber link in the network. The high capacity link networks have the drawback that single failure lead to the loss of a large amount of data. So its duration must be shorter as soon as possible.

The protection strategic increases the operation costs of the network overall, however it may reduce the most quality-related problems and constitute a specification of quality in service-level agreements (SLAs). A service-level agreement is a part of a service contract where the level of service is formally defined. In practice, the term SLA is sometimes used to refer to the contracted delivery time (of the service) or performance. It is a measure of performance from network perspective. So it is requirement of the end user.

Following the recent evolution in technology, many service providers of IP based networks start or plan to start providing one service package with video, voice and data services. It is

because IP market is becoming increasing important and a unified service platform reduce the costs and introduce new services.

In this study examined the approach of a survivable WDM mesh network with IP traffic with wavelength conversion. The nature of IP traffic is bursty. The approach is based on a basic survivable paradigm of the 1+1 dedicated protection. So the usefulness of the algorithm to study the network performance is showed.

The line bit rates of 512kb and 2048 kb are bit rates that are used widely today in the Internet. The other bit rates from 10, 100, 1000 and 10000 megabits per second (Mbit/s) show the gradual passage to higher bit rates.

The measurement of the traffic is very important because it is essential to measure the traffic for cost reasons and to monitor the user behavior.

REFERENCES

[1] H. Kobayashi. *Modeling and Analysis.* ADDISON-WESLEY 1981.

[2] F.L.Bauer et al. *Software Engineering An Advanced Course.* SPRINGER – VERLAG, 1973.

[3] V. Ahuja. *Design and Analysis of ComputerCommunication Networks* . McGRAW HILL ,1982

[4] T. Wu. *Fiber Network Service Survivability*. ARTECH HOUSE ,1992.

[5] A. Bononi.*Optical Networking* . Part 2,SPRINGER ,1992.

[6] Y. Ye, C. Assi, S. Dixit, M. A. Ali. "A Simple Dynamic Integrated Provisioning / Protection Scheme in IP over WDM Network,*" IEEE Comms Magazine*, November 2001, Vol 39, No 11, pp 174-181.

[7] O. Gerstel and R. Ramaswami, Xros. "Optical Layer Survivability-A services perspective," *IEEE Comms Magazine* March 2000,Vol 38,No 3 ,pp104-113.

[8] O. Gerstel and R. Ramaswami, Xros. "Optical Layer Survivability-An implementaion perspective*,"IEEE JSA of Communication* ,October 2000,Vol 18,No 10, pp1885-1889.

[9] S.Ramamurthy, L.Sahasrabuddhe, B.Mukherjee "Survivable WDM Mesh Networks ," *IEEE Journal of LightWave Technology*, April 2003, Vol 21, No 4, pp 870-889.

[10] I. Neokosmidis, T. Kamalakis and T. Sphicopoulos. "Accurate estimation of the impact of IP traffic burstiness on the performance of WDM networks " OPTICS EXPRESS 9702 , November2005 ,Vol 13, No 24.

[11] T.Eido, F. Pekergin, M.Marot, T.Atmaca. "Multiservic Optical Packet Switched Networks:Modeling, Performance Evaluation and QoS Mechanisms in a Mesh Slotted Architecture", Fifth International Conference on Networking and Services, Valencia, Spain, April 2009.

[12] J. Burbank "Modeling and Simulation: A practical guide for network designers and developers", *IEEE Comms Magazine*, March 2009,Vol 47, No3 , pp 118.

[13] J.Y.Choi S.H. Kwak, M.J. Lim, M.T. Chae, B.K. Shim and J.H. Yoo. "Service Traffic Management System for Multiservice IP Networks: Lessons Learned and Applications*," Communications Magazine*, April 2010, Vol 48, No 4, pp 58-65.