The GMPLS Controlled Optical Networks as Industry Communication Platform

Janusz Korniak

Abstract—**In this paper, Generalized Multiprotocol Label Switching (GMPLS) controlled optical networks are considered as industry communication network. GMPLS is a Next-Generation Network technology which will be used to build new Internet backbone. Thanks to the features of a new public network, Internet can become a platform for industrial communication including critical data, transactional flow, and real-time data. The benefits of such a network for industry are explained in this paper. Next, the idea and architecture of intelligent, next-generation optical transport networks is discussed and explained. One of the challenges of GMPLS technology is a reliability as the main factor which influences service quality. Therefore, the method of improving reliability of GMPLS is proposed. This method bases on the implementing of redundancy in the control plane. Using Monte Carlo simulation and proposed reliability analysis method quantity improvement of GMPLS network reliability is shown and the merits of using this method are confirmed. Achieved simulation results and analysis confirm also that this emerging optical transport network will offer industry long distance communication with transmission condition compared to what is provided by dedicated WAN links. Simultaneously using public infrastructure can reduce cost of long distance communication.**

Index Terms—**Automatically switched optical network (ASON), generalized multiprotocol label switching (GMPLS), industrial control system, Monte Carlo simulation, optical transport networks, real-time communication, reliability.**

I. Introduction

THE CONTINUOUS growth of traffic flow in the Internet and more sophisticated services are the challenges for future network backbone of the Internet. Increased volume of Internet traffic is compromised by optic transmission technologies and media. At the same time, new services forced to overcome the limitations of the best effort approach in IP networks.

Industry needs robust platform for distributed system communications. Many works are devoted to adapting existing technology like Ethernet [1] or Wi-Fi networks [2]. Another trend is to develop dedicated industry networking technology. For example, Real-Time Ethernet [3] is such a solution. In many cases, systems need dedicated or specially conditioned communication platform. However, in some cases, systems could use public communication networks. Especially, when distances between remote subsystems require to use wide area network solutions [4].

Since the Internet network has been more reliable than even before, it will able to become the platform for industry control and real-time communication. Of course, broadband access networks are necessary to connect the customer to the public network. Technologies like Fiber-to-The-Home (FTTH) or Fiber-to-The-Building (FTTB) generally called Fiber-to-The-x (FTTx) allow customers and service providers to build all-optical high-speed connections. The Next-Generation Networks (NGN) will satisfy industry requirements for distributed systems and will open new opportunities.

A. Next-Generation Networks

Traditional optical networks are too complex to build dense, mesh optical networks. A simplification trend is observed. Of course, DWDM technologies will be widely implemented to support high bandwidth of transmission. However, switching of the traffic by network nodes is a bottle neck of communication performance. The IP switching in the backbone networks must be reduced due to excessive delay and cost. The layer 2 switching is not a forward-looking method. Therefore, optical switching must be widely implemented. For this reason, self-organizing optical networks is to be developed. The Automatically Switched Optical Network (ASON) [5], promoted by ITU-T is such a technology.

The limitations of the best effort IP networks are overcome by implementation of quality of services. Especially, two QoS models become dominant, Differentiated Services (DiffServ) and Integrated services (IntServ). However, there are many other optimization methods avoiding congestion in the network and transmission improving of time-sensitive traffic, for example, [6]. While the DiffServ model is widely implemented in IP networks, more sophisticated traffic engineering methods for optical backbone network are needed. The Generalized Multiprotocol Label Switching (GMPLS) [7] is emerging technology developed to support traffic engineering and satisfy mentioned requirements.

B. Benefits for Industry

The GMPLS controlled optical networks will be beneficial for service providers and industry. From the viewpoint of the industrial customer, several features are the most important.

1) Fast provisioning of services.
2) Ensuring a high level of service.
3) Cost-effective subsystem communication.
4) Easiest access to optical backbone.

The first feature enables the industry to require on-demand services which can be established within minutes or seconds. This is especially interesting when customers occasionally need to

Manuscript received February 05, 2011; revised May 23, 2011; accepted June 09, 2011. Date of publication September 06, 2011; date of current version November 09, 2011. Paper no. TII-11-048.

The author is with the Department of Electronics and Telecommunications, University of Information Technology and Management, Rzeszow 35-225, Poland (e-mail: jkorniak@wsiz.rzeszow.pl).

Digital Object Identifier 10.1109/TII.2011.2166776

1551-3203/$26.00 © 2011 IEEE

send very large package of data or maintain video teleconference with other partners or remotely control delegated system.

The second feature ensures high availability, low delay and jitter, reserved bandwidth, and other parameters. High availability can be provisioned in expected levels through the recovery mechanisms offered by GMPLS networks. Thus, customer traffic can be restored or protected in a variety of ways to give sufficiently low probability of transmission interruption and short time of transmission loss. This creates new opportunity for industry to transfer critical data. For example, Internet backbone can be used to transfer signaling traffic which control remote industry operations. The traffic engineering methods used in GMPLS network can also ensure other transmission parameter to support industry requirements on appropriate level at this time.

Remote control for long distances can be very expensive when dedicated communication infrastructure must be created. It is commonly known that the main cost of wide area networks is the link between remote locations. Therefore, using of the GMPLS tunnel over public infrastructure will be a cost-effective solution. Together with fast provisioning and high level of services GMPLS tunnels can become popular in the industry due to benefits offered by this technology.

The GMPLS controlled optical networks support scalability and flexibility. Thanks to this, the service providers can build dense optical backbone networks with more nodes. In this way, they can be available in places where the optical transport network is not available at present.

For example, imagine that the company received an order for a task by his robot in a remote location. A robot to perform ordered task needs to be controlled by a master system located in the central office and communicate with other subsystems in different locations. Necessary communication includes control signals, video stream, and other data. For this reason, company requests temporary, on demand transmission connection with demand parameters necessary for subsystem communication. Requested communication parameters can include reserved throughput, minimum delay and jitter, and desired level of service availability. After finishing a tasks requested connection can be released.

Currently, using traditional technology and available resources it may be difficult to do. The company may encounter the following problems.

- Access network to remote location has insufficient bandwidth.
- Service provider in remote location may need several days to provide broadband connection.
- Service provider in remote location may not guarantee required service level to central office.
- End-to-end connection between remote location and central office may be operated by several service providers.
- Service provider may refuse service because of its unprofitability for such short time.

Transport networks extended based on GMPLS can provide abilities to perform this task.

In order to guarantee high level of services, appropriate industry application GMPLS network has to be reliable. This is one of the challenges of wide area industry communication.

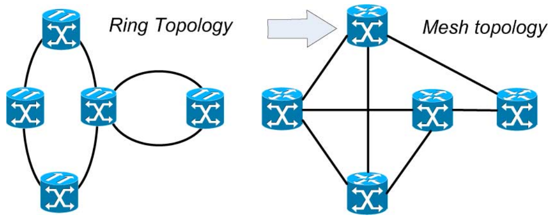


Fig. 1. Ring topology of traditional optical networks (left side and mesh topology of emerging transport networks (right side).

II. GMPLS Controlled Optical Networks

A. Protocols and Standardization

Currently, two concepts ASON and GMPLS are developed separately by ITU-T and IETF, respectively. But both have the same goal: to enable intelligent, self-organizing optical transport network. Traditional optical networks are based on ring topology, see Fig. 1. Emerging optical networks assume mesh topology with many nodes and connections. In such networks, signaling and routing is a challenge when compared to traditional ring networks.

The ITU-T G.7713/Y.1704 recommendation specifies three distributed call and connection management methods.

- PNNI/Q.2931.
- GMPLS RSVP-TE.
- GMPLS CR-LDP.

Thus, ASON networks can use GMPLS methods as the control plane signaling method. However, the IETF MPLS working group deprecated CR-LDP and focus on Resource Reservation Protocol - Traffic Engineering (RSVP-TE) [8]. Therefore, this protocol seems to be preferable signaling method for emerging ASON networks.

While preferable call and connection signaling protocol is chosen, the method for path Label Switched Path selection still is open. Of course, link-state routing protocols are available but must be extended to support traffic engineering and specifics of optical networks like protection path. For example, works [9] and [10] mention this problem.

B. Network Architecture

Traditionally, operation of the telecommunication networks is divided into three logical, functional planes (see Fig. 2).

- **Data plane** is responsible for transmission of user data. It includes all switching techniques such as WDM, TDM, packet switching, etc.
- **Control plane** is responsible for exchanging signaling and routing messages. It is implemented as IP network that supports protocols known from MPLS such as LDP, RSVP, OSPF, and their traffic engineering extension.
- **Management plane** is responsible for management of whole system; it may be implemented as centralized or distributed system that allows to employ provider's policy.

One of the most important assumptions for ASON or GMPLS controlled optical networks is all-optical switching. It means that user data traffic injected into optical network domain is switched optically without opto-electro-opto conversion. However, the signaling traffic cannot be forwarded in this way because IP content of traffic flow is not accessible by nodes. The

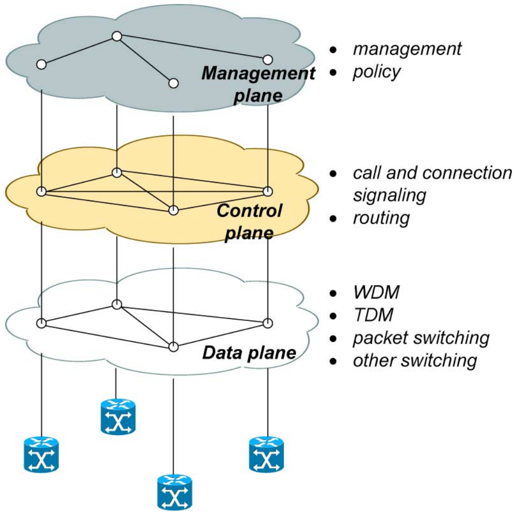


Fig. 2. Functional planes of GMPLS network.

consequence of this assumption is physical separation of functional planes and out-of-band or even out-of-fiber signaling. Functional planes separation has impact to the network operations. For example, this problem is considered in [11]. There are two main considerations which are studied:

- symmetry or asymmetry of topology;
- dependability of physically separated functional planes.

Both are mentioned in the context of a network reliability. Symmetry occurs when topologies of data and control planes are identical. Otherwise, a network is asymmetric. Fig. 2 presents asymmetrical network because the control plane has more connections than the data plane. Asymmetric network can be a result of network element failure or can be intentionally planned [11] for achieving better reliability. Dependability between functional planes is also a very important issue because operation of the data plane depends on the operation of the control plane [12].

C. GMPLS Network Operations

The Fig. 3 shows an example network for which on-demand tunnel called Label Switched Path (LSP) should be established between nodes LSR1 and LSR6. There are three steps to set up LSP:

1) path computing;
2) path establishing;
3) resource allocation.

The route selection is determined by routing information. If OSPF routing protocol with Traffic Engineering extension [13] is used, topology information reflects currently reserved bandwidth and selected path has available resources for requested new LSP. When the path is determined the reservation process can start. RSVP-TE protocol sends from LSR1 *Path* message along determined path to LSR6 and when reach destination *Resv* message from LSR6 back to LSR1. Thus, LSP is established and recourses are allocated. From now the LSR1 can accept data flow and optically switch toward the destination.

Another important signaling task is a failure maintenance. Recovery mechanism bases on signaling messages used to inform ingress and egress LSR. After a failure is detected and localized notification message is send to ingress LSR. Depending on used recovery methods ingress LSR performs appropriate operations to prepare new LSP or to switch to preallocated backup LSP.

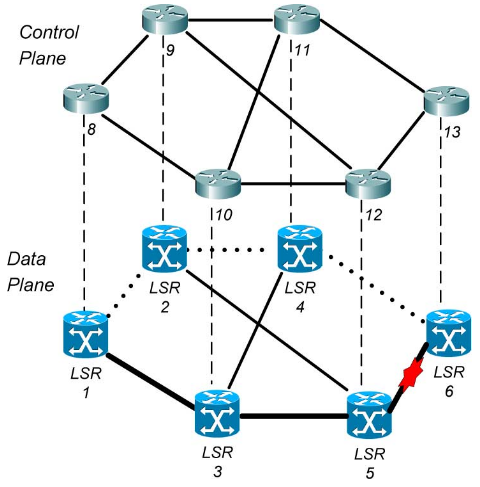


Fig. 3. Sample GMPLS network with working LSP (bold line) and protection LSP (dotted line).

III. Reliability of GMPLS Network

The reliability of GMPLS controlled optical networks becomes an issue because the backbone of new generation Internet will be the platform for new industry services characterized by a need of very high availability.

A. Reliability Parameters

The reliability of telecommunication system is defined as ‘the probability that an item can perform a required function under stated conditions for given time interval” [14]. It can be classified to:

- two terminal reliability—known also as source-target reliability;
- all terminal reliability.

From the point-of-view of the end-to-end services, the first method is suitable because expresses that path between source and target is operational. However, from perspective of telecommunication operator all terminal reliability should be considered.

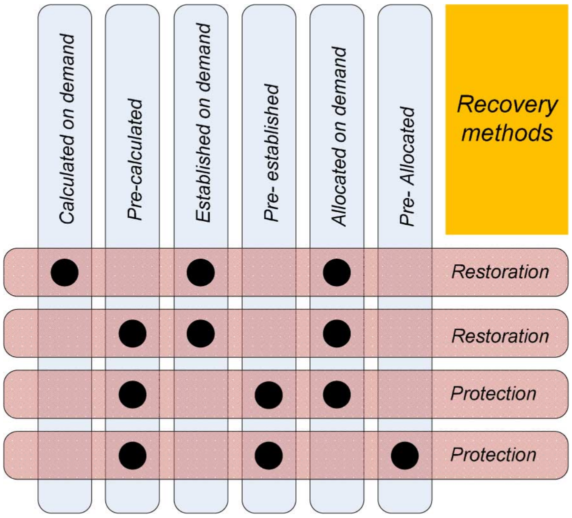
There are two main statistic parameter used in reliability engineering.

- Mean Time To Failure (MTTF)—the average time between failures of hardware or software module.
- Mean Time To Repair (MTTR)—the average time taken to repair a failed hardware or software module.

Another parameter frequently used to describe reliability is an availability (A) defined as

$$A = \frac{\mathrm{MTTF}}{\mathrm{MTTF} + \mathrm{MTTR}}. \tag{1}$$

Thus, in order to increase availability of system, MTTF should be maximized and/or MTTR should be minimized. A network is a complex interconnected system with components characterized by individual MTTR and MTTF parameters. Reliability of such system can be improved in many ways.



Calculated on demand	Pre-calculated	Established on demand	Pre- established	Allocated on demand	Pre- Allocated	Recovery methods
●		●		●		Restoration
	●	●		●		Restoration
	●		●	●		Protection
	●		●		●	Protection

Fig. 4. Recovery set up methods.

B. Survivability

The network is naturally survivable system providing many alternative paths between source and destination. In IP networks routing process is responsible for maintenance this task. In the case of GMPLS controlled optical networks, traditional routing is not enough. An alternative path is calculated after routing convergence which takes too long a time for backbone, optical network. Therefore, additional mechanisms are implemented.

The main method for achieving very high availability of transmission services offered by GMPLS controlled optical network is a path recovery. There are several recovery options which lead to find alternative LSP to bypass traffic from failed LSP. The backup LSP can be calculated on-demand or precalculated, established on-demand or preestablished and resources can be allocated on-demand or preallocated. Recovery methods are summarized in Fig. 4. Suppose that in the network presented on Fig. 3, the link between LSR5 and LSR6 fails. If new path is computed on-demand transmission service unavailability is a sum of:

- failure detection and localization time;
- notification of LSR1 delay;
- path computation delay;
- path establishing - *Path* message propagation and processing delay;
- path reservation - *Resv* message propagation and processing delay;
- switching to new LSP delay.

This restoration method may not be enough for customer needs, therefore, the alternative LSP can be precomputed, preestablished, and preallocated. In this case, protection of LSP occurs. For example, if LSP marked by bold lines is protected by preestablished and preallocated LSP marked by dotted lines, transmission service is recovered in the following steps:

- failure is detected and localized;
- LSR5 notifies LSR1 about failure;
- LSR1 informs LSR6 that the traffic is switched to protection LSP.

In this way, recovery time is reduced mainly to the delay of signaling messages propagation between point of failure and ends of recovery LSP.

If distance between ingress LSR and egress LSR is long, segment recovery can be more effective than end-to-end recovery mentioned above. In the network from Fig. 3 main LSP, marked by bold lines can be protected by two segments: LSR1-LSR2-LSR5 and LSR3-LSR4-LSR6. When failure of link between LSR5 and LSR6 occurs LSR5 sends notification to LSR3 where the traffic is switched to recovery segment. Thus, the switching delay is reduced because point of repair is closer than ingress LSR used to switch-over of the traffic in the case of end-to-end recovery.

The protection method in which data flow is forwarded by working LSP while protection LSP is preallocated and ready to use in the case of failure is called 1:1 method. However, another method called 1+1 can also be used. This method assumes simultaneous data transmission over both two LSPs. Thus, in this case, the highest level of resiliency is achieved. When a failure occurs in one LSP data is still transmitted over the second LSP without any interruption.

In this way, the MTTR time can be minimized to expected level increasing availability of network services. However, these operations require intensive signaling traffic and storing of state information by network nodes. Computation of the path needs routing information, establishment of the path requires call connection signaling, resources allocation uses reservation messages. Therefore, the control plane reliability has key impact to the overall GMPLS network reliability [15].

C. Control Plane Reliability

The control plane and data plane are disjoint networks but the operation of the data plane strongly depends on the control plane reliability. A failure in the control plane can cause a loss of signaling message or state information what affects data transmission. Therefore, improving reliability of the control plane is key research goal.

Typical response of the network to a failure in the control plane is to launch recovery procedures adequate for the failure of corresponding component in the data plane. For example, a failure of the control plane link is treated as a failure of the link in the transport plane. Similarly, the failure of the control plane software (for example, RSVP-TE) is interpreted as a failure of the whole node (with the OXC module). Therefore, recovery procedures for the control plane is expected and developed.

The restoration of a state information after a failure of the control plane component can preserve the data plane operations and the control plane operations can be recovered. The IETF recommendation defines the graceful restart extensions to GMPLS (RSVP) [16], which concerns the recovery of the restarted nodes. Another way, proposed by author, to improve reliability of the control plane is the protection of signaling channels. The signaling channel, typically a link between the control plane nodes, is protected by alternative signaling path between these nodes [17]. The main idea of this approach is to prepare the alternative signaling path. This backup path should be established and ready to use in the case of a failure in the primary signaling path.

The best resilience of the control plane provides redundancy of its components. In this approach, both the control plane nodes and signaling channel are redundant. The idea of this mechanism satisfies the 1+1 packet protection suggested by ITU-T for ASON in the G.7712 recommendation [18].

In the next section, high reliability of GMPLS controlled optical networks is proved by the simulation.

IV. Simulation Analysis of the Impact of Control Plane Redundancy to the Reliability of GMPLS Network

The reliability analysis can be performed in the context of offered services. The protection and restoration in the data plane provides high level of service availability, however, it is costly for network operator because it must ensure additional resources for backup paths. This cost is especially high when path protection with resources preallocation is used. In this case, reliability of the control plane is especially important. Therefore, analysis of the influence of the control plane redundancy is performed in the network with the limited resources.

A. Reliability Evaluation

The reliability evaluation of the GMPLS controlled optical network requires special approach. Therefore, author proposed to treated GMPLS controlled optical network as a multistate system. The Label Switched Path (LSP) can have more than only two “up”and “down” states, other called “derated” is also possible. The “up” state occurs when there are no failures in a network. The “down” state means that working LSPs are failed and backup LSPs cannot be used. The “derated” state occurs in all other cases for example, primary LSP failed but protection LSP works or primary works but protection failed. Considering all terminal reliability, the following states can be recognized:

- “up”—No failure.
- “derated 1”—Failure occurs but has no impact to the data plane operations.
- “derated 2”—Failure occurs and starts protection mechanisms, all traffic flows are preserved.
- “derated 3”—Failure occurs, all traffic flows are preserved but some LSP losses its protection.
- “derated 4”—Failure occurs, but lack of resources causes that some LSP are not preserved.
- “down”—All services are unavailable.

Within these states the first one is mostly desirable however, probability of derated states is significant. Decreasing of this probability is possible by improving the control plane reliability. The following simulation verifies probability of derated states when redundancy of the control plane is implemented.

B. Simulation

There are many network reliability evaluation methods, including [19]:

- reliability block diagramming;
- state enumeration;
- Monte Carlo and discrete-event simulation.

For mentioned purposes, Monte Carlo-based simulation is applied. The simulation is performed according to the following steps:

1) set the input parameters;
2) generate flows information: working LSPs and backup LSPs;
3) start simulation, gather statistics, and state information;
4) analyze state information for different control plane implementations.

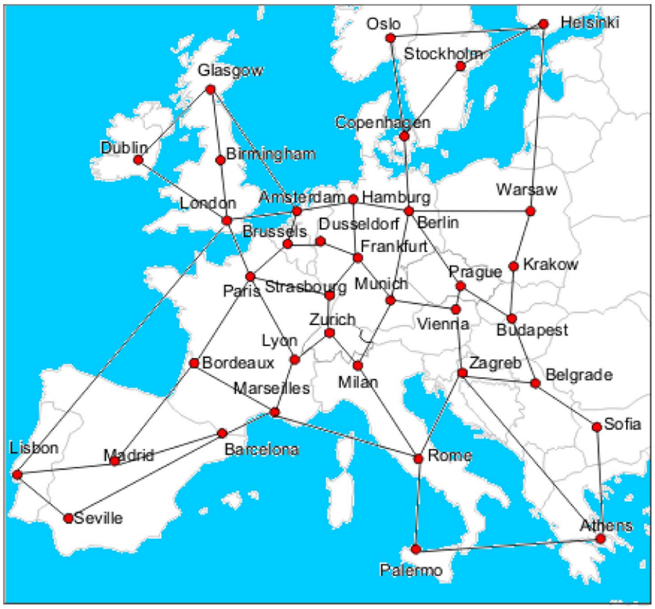


Fig. 5. Cost266 network used in the simulation.

This simulation has been implemented by author in Scilab environment with the use of Metanet module [20].

1) Input Parameters for the Simulation: This experiment is performed on the reference network cost266 [21], see Fig. 5, for which limited number of LSPs for each link is allowed. Each of the network component can suffer a failure. In presented the simulation experiment Markov process is assumed. Therefore, time between failures and time to repair are modeled by exponential distribution

$$f(T) = \lambda e^{-\lambda T} = \frac{1}{m} e^{-\frac{1}{m}T} \tag{2}$$

where $T \geq 0, \lambda > 0, m > 0$ and:

- λ is the constant failure rate;
- m is MTTF or MTTR.

Typical values of MTTF and MTTR can be obtained from literature, examples [22] and [23]. A traffic flows between randomly distributed sources and destinations are assumed. Additionally, all working LSPs are protected using dedicated (1:1) or shared (N:M) methods. The values of simulation input parameters are summarized in the Table I.

2) Working and Backup LSPs: Working LSPs are generated by random selection, according to uniform distribution, source and destination nodes. Then, constrained shortest path first algorithm is used to calculate working LSPs and include reserved bandwidth according to [13]. Some of working LSPs are protected by dedicated (1:1), disjoint end-to-end backup LSPs. Others of working LSP will be restored in the case of failure. To calculate backup LSPs, the same algorithm is used with the difference that links and nodes included in working LSP are excluded from a network graph. Example of distribution of link reservation obtained using this approach is shown in Fig. 6.

3) Simulation and Information Gathering: In this stage of prepared simulation experiment has been started with assumed

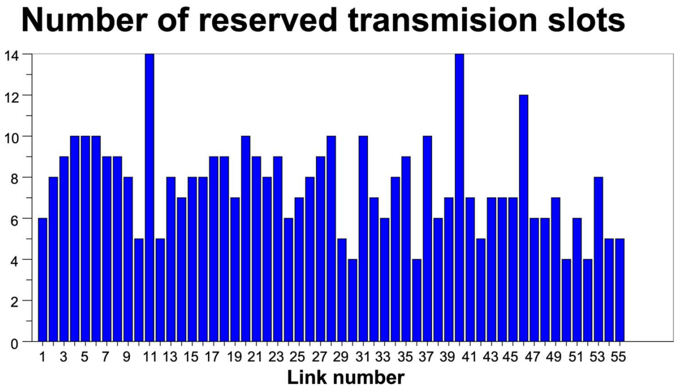


Fig. 6. Distribution of link reservation in the network.

TABLE I
THE INPUT PARAMETERS FOR THE SIMULATION

Parameter	Value
MTTF of OXC	60 000h
MTTR of OXC	4h
MTTF of data plane link	10^5h
MTTR of data plane link	12h
MTTF of router	25 000h
MTTR of router	2h
MTTF of control plane link	10^5h
MTTR of control plane link	12h
Number of working LSPs	74
Percentage of LSPs protected with 1:1 method	20
Limit of LSPs for particular data plane link	14 - 17
Number of Monte Carlo iterations	10^6

parameters summarized in Table I. For each iteration of simulation failed components are listed for further analysis.

4) Analysis of State Information for Different Control Plane Implementations: The influence of recorded failures on the network operations is considered depending on three cases of redundancy in the control plane:

- redundant the control plane channel—case A;
- redundant the control plane channel and nodes—case B;
- redundant the control plane nodes—case C.

The case with no control plane redundancy is also taken into account—case 0. A state of network is analyzed for each failure or set of simultaneous failures and according the method described in Section IV-A probabilities of derated states has been calculated.

C. Simulation Results

The evaluated estimator of probability that the network is in any derated state is equal to 0.0173 with relative error equal to 0.75%. During all simulations, "down" state did not occur. Tables II–IV include the results of analysis when transmission slots per link is limited to 14, 15, and 16, respectively. The values in tables represent percentage distribution of derated states caused by a failure or failures.

The influence of the control plane redundancy can be concluded based on the analysis between cases 0, A, B, and C. The differences between tables allow to include the limitation of networks resources in analysis.

TABLE II
PERCENTAGE DISTRIBUTION OF DERATED STATES FOR TRANSMISSION SLOTS LIMITED TO 14 PER LINK

Case	derated1	derated2	derated3	derated4
0	0.	6.4450867	35.387283	58.16763
A	35.682081	3.3468208	17.878613	43.092486
B	49.878613	3.3699422	17.965318	28.786127
C	14.196532	6.4682081	35.473988	43.861272

TABLE III
PERCENTAGE DISTRIBUTION OF DERATED STATES FOR TRANSMISSION SLOTS LIMITED TO 15 PER LINK

Case	derated1	derated2	derated3	derated4
0	0.	46.774566	24.867052	28.358382
A	35.682081	23.768786	12.410405	28.138728
B	49.878613	23.895954	12.468208	13.757225
C	14.196532	46.901734	24.924855	13.976879

TABLE IV
PERCENTAGE DISTRIBUTION OF DERATED STATES FOR TRANSMISSION SLOTS LIMITED TO 16 PER LINK

Case	derated1	derated2	derated3	derated4
0	0.	71.543353	0.0982659	28.358382
A	35.682081	36.144509	0.0346821	28.138728
B	49.878613	36.32948	0.0346821	13.757225
C	14.196532	71.728324	0.0982659	13.976879

Based on presented results the following statements are true.

1) Redundancy of the Control Plane Improves Resiliency of a Network: The higher values in columns "derated 1" and "derated 2" for cases A, B, and C than for case 0 confirm this fact because states "derated 1" and "derated 2" are more desired than "derated 3" and "derated 4." This regularity is observed in all three tables.

2) Redundancy of Both Channels and Nodes Is Most Effective: When channels and nods are redundant almost 50% (49.878613%) of failures cause shift to "derated 1" state which is the most desired after "up" state. Further analysis confirm that in the case B the control plane is almost fully resilience.

3) Redundancy of the Control Plane Channels Is Especially Important When Resources are Limited: When resources are not an issue (Table IV) redundancy of the control plane channels avoids to start protection in the case of failure of the control plane link. Value 36.144509 decreased from 71.543353 in column "derated 2" and value 35.682081 increased from 0 in column "derated 1" and confirms this fact. However, values representing states "derated 3" and "derated 4" are on similar level in case 0 and case A. When resources are more limited (Table II) values representing states "derated 3" and "derated 4" are significantly smaller in case A than in case 0. This fact confirms additional benefit of this redundancy.

Presented simulation has been repeated for different flow patterns and different input parameters. The results of these simulations confirm above statements. However, numerical values are omitted in this paper to avoid its overloading.

V. Discussion

The simulation results confirm usefulness of the control plane redundancy. However, technical and economic analysis of proposed solution should be preformed.

A. Technical Aspect of the Control Plane Redundancy

The are two aspects of implementing redundancy of the control plane. The first one concerns signaling redundancy and the second router redundancy.

The most important for the GMPLS network operation is signaling protocol. As mentioned in Section II-A, RSVP-TE is the preferred method for GMPLS. Typically, RSVP messages are exchanged between directly connected nodes. However, for signaling redundancy, Node-ID Based RSVP [24] is more suitable. In this approach, messages are exchanged between logical interfaces defined on nodes. Thus, in the case of a failure of direct link between nodes, alternative connection between nodes, identified by node-id can be established. This approach also supports 1+1 protection of signaling traffic. Duplicated messages can be forwarded over two disjoint signaling paths. Implementation of such redundancy is possible. Alternative signaling channel can be established with the use of some tunneling protocol like MPLS. Processing of duplicated RSVP-TE messages does not require modification of RFC recommendations. Duplicated messages are treated as refreshment or are ignored.

The redundancy of the control plane router is more difficult than redundancy of signaling channel. Only one of the control plane routers can perform control of the data plane operations, while the second has to be ready to take over function of the first one. Moreover, both routers must exchange state information and monitor operations performed by each other. Implementation of such redundancy is possible. An example of mentioned requirements to router redundancy is described in [25]. Of course, Virtual Router Redundancy Protocol (VRRP) considered in this document offers redundancy of default gateway for LANs but many of the used solutions can be adapted to the redundancy of the control plane router.

B. Economic Aspect of the Control Plane Redundancy

The cost of the implementation of the control plane redundancy is moderate. Redundancy of the signaling channel is implemented in software, no investment in hardware is necessary. The main cost is related to the control plane router redundancy. Developing cost of redundant routers hardware can be high due to technical requirements mentioned in previous subsection. But profits resulting from the application of the control plane redundancy can balance financial outlays. Especially, only the most important links and nodes in the control plane can be selected for implementing redundancy.

Based on achieved simulation results, it is possible to estimate average time of derated states for the network for one year of operation. Because probability that the network is in a derated state, is equal 0.0173 (the result of simulation). It means that the network is under suboptimal operation during approximately 151.5 h. In the absence of the control plane redundancy and when resources are limited, the network uses additional resources or cannot provide all services. When redundancy of routers and control plane channels is applied only on half of this time (75 h) the network is in that unfavorable state. That estimation can be used to analyze profits and investments.

VI. Conclusion

The Internet public network becomes the common communication platform for many applications. The main reason of this trend is the cost reduction of using dedicated, private network. An evident example of converged network is the Internet. One particularly noteworthy phenomenon is the Virtual Private Network (VPN), technology with open public network infrastructure for private business. Emerging optical technologies like GMPLS controlled optical networks will provide survivable and intelligent networks which will offer very high-quality services and open public network for industry communication on a large scale.

It is especially interesting for long distance communication, where wide area network technology must be used. Because long distance network infrastructure is very expensive using public next-generation backbone network will be cost effective. Key features of GMPLS controlled optical transport network guarantee transmission conditions compared to those provided by dedicated (leased) WAN links. Moreover, it offers global connectivity over the world.

Some of the industry processes are limited to local area because required data communication for mission critical information are supported only locally. GMPLS networks due to their reliability enable distributed industry processes for long distances. The results of presented simulations confirm that this network can offer very high reliability expected in industry applications.

References

[1] J. Ploennigs, M. Neugebauer, and K. Kabitzsch, “Diagnosis and consulting for control network performance engineering of CSMA-based networks,” *IEEE Trans. Ind. Inform.*, vol. 4, no. 2, pp. 71–79, May 2008.

[2] M. Jonsson and K. Kunert, “Towards reliable wireless industrial communication with real-time guarantees,” *IEEE Trans. Ind. Inform.*, vol. 5, no. 4, pp. 429–442, Nov. 2009.

[3] J. Jasperneite, J. Imtiaz, M. Schumacher, and K. Weber, “A proposal for a generic real-time ethernet system,” *IEEE Trans. Ind. Inform.*, vol. 5, no. 2, pp. 75–85, May 2009.

[4] Q. Wang and S. Gopalakrishnan, “Adapting a main-stream internet switch architecture for multihop real-time industrial networks,” *IEEE Trans. Ind. Inform.*, vol. 6, no. 3, pp. 393–404, Aug. 2010.

[5] A. Jajszczyk, “Automatically switched optical networks: Benefits and requirements,” *IEEE Commun. Mag.*, vol. 43, no. 2, pp. S10–S15, 2005.

[6] T. Bartczak, S. Paszczynski, and B. M. Wilamowski, “Improvement of the computer network transmission band usage by packing agent technology,” in *Proc. 3rd IEEE Int. Conf. Ind. Inform.*, 2005, pp. 384–389.

[7] E. Mannie, “Generalized multi-protocol label switching (GMPLS) architecture,” RFC3945, 2004.

[8] A. Farrel, Ed., “Inter-domain MPLS and GMPLS traffic engineering—resource reservation protocol-traffic engineering (RSVP-TE) extensions,” RFC5151, 2008.

[9] A. Haider and R. Harris, “Recovery techniques in next generation networks,” *IEEE Commun. Surveys Tutorials*, vol. 9, no. 3, pp. 2–17, 2007.

[10] M. P. Pioro, A. Tomaszewski, C. Zukowski, D. Hock, M. Hartman, and M. Menth, “Optimized IP-based vs. explicit paths for one-to-one backup in MPLS fast reroute,” in *Proc. 14th Int. Telecommun. Network Strategy and Planning Symp. (Networks 2010)*, 2010, pp. 209–214.

[11] P. Rozycki and A. Jajszczyk, “The weighted graphs approach for the GMPLS network reliability enhancement,” in *Proc. 2nd Int. Workshop on Reliable Networks Design and Modeling (RNDM 2010)*, 2010, pp. 135–141.

[12] P. Rozycki, J. Korniak, and A. Jajszczyk:, "Failure detection and notification in GMPLS control plane," presented at the IEEE ICC 2007, the Workshop on GMPLS Performance Evaluation: Control Plane Resilience, 24, Glasgow, Jun. 2007.

[13] D. Katz, K. Kompella, and D. Yeung, "Traffic engineering (TE) extensions to OSPF version 2," RFC 3630, 2003.

[14] "Terms and definitions related to quality of service and network performance including dependability," 1994, ITU-T, Recommendation E.800.

[15] A. Jajszczyk and P. Rozycki, "Recovery of the control plane after failures in ASON/GMPLS networks," *IEEE Network*, vol. 20, no. 1, pp. 4–10, 2006.

[16] A. Satyanarayana and R. Rahman, "Extensions to GMPLS resource reservation protocol (RSVP) graceful restart," RFC 3473, 2007.

[17] J. Korniak and P. Rozycki, "Service availability analysis of GMPLS network," in *Proc. 14th Int. Telecommun. Network Strategy and Planning Symp. (Network 2010)*, Sep. 27–30, 2010, pp. 292–296.

[18] "Architecture and specification of data communication network," 2010, ITU-T, Recommendation G.7712/Y.1703.

[19] M. Sahinoglu and B. Rice, "Network reliability evaluation," *Comput. Statistics*, vol. 2, no. 2, pp. 189–212, 2010.

[20] *Metanet Project,* 2010. [Online]. Available: http://forge.scilab.org/p/metanet

[21] *SNDlib library,* 2011. [Online]. Available: http://sndlib.zib.de

[22] I. Rados, "Availability analysis and comparison of different WDM systems," *J. Telecommun. Inform. Technol.*, vol. 2, pp. 114–119, 2007.

[23] M. To and P. Neusy, "Unavailability analysis of long-haul networks," *IEEE J. Select. Areas Commun.*, vol. 10, no. 1, pp. 100–109, 1994.

[24] Z. Ali, R. Rahman, D. Prairie, and D. Papadimitriou, "Node-ID based resource reservation protocol (RSVP) hello: A clarification statement," RFC 4558, 2006.

[25] S. Nadas, Ed., "Virtual router redundancy protocol (VRRP) version 3 for IPv4 and IPv6," RFC 5798, 2010.

Janusz Korniak received the M.S. degree in 1997 from Rzeszow University of Technology, Rzeszow, Poland, in 1997 and the Ph.D. degree in telecommunication engineering from the University of Technology and Agriculture, Bydgoszcz, Polandm in 2005

Since 1997, he has been working at the University of Information Technology and Management (UITM) as a Teaching and Research Assistant in the Department of Electronics and Telecommunications. Currently, he works at UITM as an Associate Professor. He is the author of numerous scientific publications in this field. His current research focus on reliability of optical transport networks.