UDK: 621.395.74: 004.03
COSATI: 17-02, 15-03

GMPLS-next generation solution for IP switching through military heterogeneous networks

Dragan Ilić, BSc (Eng)[1)]
Milan Lazarević, BSc (Eng)[2)]
Marinko Smiljanić, BSc (Eng)[2)]
Nenad Okanović, BSc (Eng)[2)]

Optical Wavelength Division Multiplexing (WDM) networking technology has been identified as a suitable candidate for future network environments, due to its potential ability to meet the rising demands of high bandwidth and low latency communication. But nowadays, network technology is very different and heterogeneous, so solution for communication in these circumstances must be able to resolve it. This paper discusses GMPLS (*Generalized Multi Protocol Label Switching*) as a potential solution and suggests possible applications in the military environment where this set of protocols can resolve the problems of several network and device types. The diversity and complexity in managing these devices have been the main driving factors in the evolution and enhancement of the MPLS (*Multi Protocol Label Switching*) suite of protocols to provide control for not only packet based domains, but also time, wavelength and space domains.

Key words: **telecommunication systems, military telecommunications, internet protocol, generalized multi protocol label switching, routing.**

Used symbols

WDM – Wavelength Division Multiplexing
GMPLS – Generalized MultiProtocol Label Switching
MPLS – MultiProtocol Label Switching
ICT – Information Communication Technology
IP – Internet Protocol
QoS – Quality of Service
IETF – Internet Engineering Task Force
RSVP – Resource reSerVation Protocol
OSPF – Open Shortest Path First
ATM – Asynchronous Transfer Mode
LSP – Label-Switched Paths
LDP – Label Distribution Protocol
BGP – Border Gateway Protocol
LER – Label Edge Routers
LSR – Label Switching Routers
PE – Provider Edge router
P – Provider Router
FEC – Forward Equivalence Class
OLS – Optical Label Switching
TDM – Time division Multiplexing
SDH – Synchronous Digital Hierarchy
SONET – Synchronous Optical Network
FDM – Frequency Division Multiplexing
OXC – Optical Cross – Connect
L2SC – Layer-2 Switch Capable
MAC – Medium Access Control
VPI – Virtual path Identifier
VCI – Virtual Channel Identifier
LSC – Lambda Switch Capable
PXC – Photonic Cross-Connection
FSC – Fiber Switched Capable
PSC – Packet Switched Capable
DSC – Digital Switched Capable
IS-IS – Intermediate System to Intermediate System
TE – Traffic Engineering
CR-LDP – Constraint based Routing – Label Distribution Protocol
OSI – Open System Interconnection
LMP – Link Management Protocol
LoL – Loss of Light
VPN – Virtual Private Network
IPSec – IP security
PPTP – Point-to-Point Tunneling Protocol
L2TP – Layer 2 Tunneling Protocol
CE – Customer Edge

Introduction

INFORMATION Communication Technology (ICT) maintenance is one of the most important military activities which are supposed to create conditions for real time battle activities.

Basic needs of military communication and information support are: voice and data transmission, protection of voice and data and electronic data processing. Network communication failure means failure of the whole military command system [1].

We have witnessed a wide deployment to enhance the IP (*Internet Protocol*) suite to support traffic engineering as well as QoS (*Quality of* Service).

[1)] NIL Communication systems, III Bulevar 25a, 11070 Belgrade, SERBIA
[2)] Military Academy, Pavla Jurišića Šturma 33, 11000 Belgrade, SERBIA

Special attention must be given to security during transfer since all parts of military connections have to be safe to use. The most complicated, and certainly the most useful ways to protect those connections is to change the protocol format, to use crypto or other security mechanisms.

MPLS fundamentals

MPLS is an Internet Engineering Task Force (IETF) – specified framework that provides for the efficient designation, routing, forwarding, and switching of traffic flows through the network [2].

MPLS specifies mechanisms to manage traffic flows of various granularities, such as flows between different hardware, machines, or even flows between different applications.

MPLS performs interfaces to existing routing protocols such as Resource reSerVation Protocol (RSVP) and Open Shortest Path First (OSPF), and integrated IP and ATM (*ATM-Asynchronous Transfer* Mode) can also be in the network (MPLS could provide a bridge between access IP and core ATM).

In MPLS, data transmission occurs on Label-Switched Paths (LSPs). LSPs are a sequence of labels at each and every node along the path from the source to the destination. LSPs are established either prior to data transmission (control-driven) or upon detection of a certain flow of data (data-driven). The labels, which are underlying protocol-specific identifiers, are distributed using Label Distribution Protocol (LDP) or RSVP or piggybacked on routing protocols like Border Gateway Protocol (BGP) and OSPF. Each data packet encapsulates and carries the labels during their journey from source to destination. High-speed switching of data is possible because the fixed-length labels are inserted at the very beginning of the packet or cell and can be used by hardware to switch packets quickly between links.

The following two types of devices participate in MPLS protocol mechanisms: Label Edge Routers (LERs) and Label Switching Routers (LSRs). Furthermore, some manufacturers (like Cisco for example) give different names regarding these types of routers: Provider Edge router (PE) for LER and Provider Router (P) for LSR [3].

An LSR is a high-speed router device in the core of an MPLS network that participates in the establishment of LSPs using the appropriate label signalling protocol and high-speed switching of the data traffic based on the established paths.

LER is a device operating at the edge of the access and MPLS networks. LERs support multiple ports connected to dissimilar networks (such as frame relay, ATM and Ethernet) and forward this traffic onto the MPLS network after establishing LSPs, using label signalling protocol at the ingress and distributes the traffic back to the access networks at the egress.

The Forward Equivalence Class (FEC) is a representation of a group of packets that shares the same requirements for their transport. All packets in such a group are provided the same treatment en route to the destination.

A label is a short fixed length physically contiguous identifier. The label identifies the path a packet should traverse and it is important to know that it has only local significance to the router. The receiving router examines the packet for its label content to determine the next hop (router maintain several routing tables regarding this problem). Once a packet has been labelled, the rest of the journey of the packet through the backbone is based on label switching. The label values are of local significance only, meaning that they pertain only to hops between LSRs. Fig.1 presents the label format.

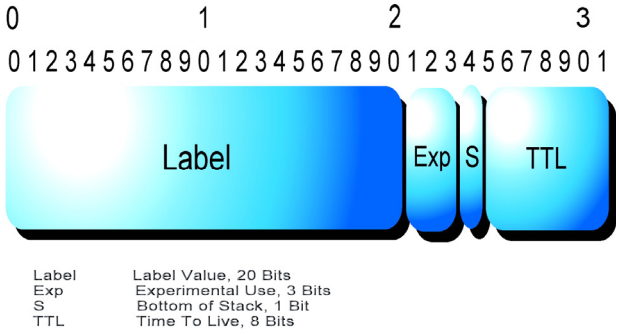
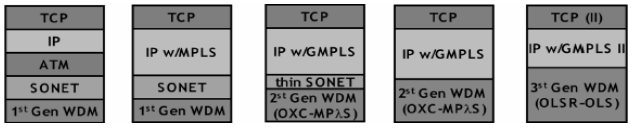


Figure 1. Label format

Talking about MPLS it can be concluded that one of the disadvantages of this protocol suite is its limitation to packet switching only. In order to provide control not only for packet transfer based domains, but for space, time and wavelength domains, a new solution arises - generalized MPLS.

GMPLS – Generalized Multiprotocol Label Switching

Huge progress in the area of traffic switching based on IP technology on one hand and high speed optical fibre usage on the other is only too obvious. GMPLS protocol as the base control level in data transfer in combination with switching at the optical level OLS (*Optical Label Switching*) may be the right decision in this kind of considerations. Evolution behind IP switching problem is very complicated but in progress; it is shown in Fig.2.



classic OSI model | MPLS and first generation of optics | GMPLS and second generaton optics | Advanced GMPLS and second generation | GMPLS II and OLS with third generation optics

Figure 2. Evolution behind IP switching problem

GMPLS provides general control plane which enables transfer and switching across various network types: packet, TDM (*Time Division Multiplexing*) and optical networks; the major challenge for creating one general control protocol which provides establishing, maintenance and traffic control toward precision paths of various types of networks with their heterogeneous domains.

The existing MPLS protocol group, which is developed by IETF, is enlarged to provide signalization and routing for all domains equipment. This general control base is trying to make network operations, management, automatic end-to-end support and network resources simpler and to provide QoS for new, more sophisticated applications.

GMPLS architecture is made from completely separated control and data array of different types of nets. The base of everything is IP routing and addresses models. This eludes using IPv4 and/or IPv6 addresses to make identification for interfaces. The traditionally distributed IP routing usage is updated to better routing protocols. GMPLS control array

technology is still IP based, but data array is becoming multiform including lots of different types of traffic (TDM, lambda, packet, optical fibre). Due to this variety, GMPLS needs to support all kinds of switching. GMPLS makes MPLS functionality much more usable due to the following:

- TDM paths where the labels are time slots (SDH/SONET (*Synchronous Digital Hierarchy/Synchronous Optical Network*) usage);
- FDM (*FDM-Frequency Division Multiplexing*) paths where the frequency is the label;
- Space multiplexed paths, where the label shows physical data position (OXC – *Optical Cross-Connect*).

The logical consequence, in order for GMPLS to satisfy links which are not packet oriented, is that the label no longer remains an abstract identification (like in MPLS and some similar solutions). The new requirement is to make it become available to map into time slots, frequencies or physical resources such as switch ports.

The problem which GMPLS set of protocols has to solve is to provide an appropriate path for potential traffic ingress in packet IP network, then to transport it through SDH/SONET domain and finally to switch it to appropriate optical fibre depending of the wavelength.

GMPLS framework needs to be considered, thoroughly including possibilities and problems: switching domain, transfer traffic type, used equipment etc. Current topic is shown in Table 1.

Table 1. GMPLS configuration architecture

Switching domain	Traffic type	Switching	Device example	Prefix
packet cell	IP ATM	label VCC (virtual channel)	IP router ATMswitch	PSC (Packet Switch Capable)
time slot	TDM	time slot	DCS* ADM**	TDM Capable
wavelength	transparent	lambda	DWDM	LSC (Lambda Switch Capable)
physical space	transparent	fibre	OXC	FSC (Fibre Switch Capable)
DCS* - Digital Cross-Connect System ADM** - Add-Drop Multiplexer				

The new LSR equipment set which is being introduced through the MPLS protocol generalization is also enlarged and is divided into [4]:

- **Interfaces that allow packet switching** – interfaces recognize the packet border and they do the data transfer depending on the packet payload context. For e.g., there are router interfaces which forward data depending on the IP header context or router interfaces which switch data depending on the little MPLS label context.
- **Interfaces that allow switching on the second layer** (*L2SC–Layer–2 Switch Capable)* – interfaces recognize frames/cell borders and can switch data depending on the frame or cell header context. Ethernet bridge interfaces supported by MAC (*Medium Access Control*) header traffic switching as well as classic ATM–LSR equipment which make ATM VPI/VCI *(ATM Virtual Path Identifier/Virtual Channel Identifier)* are concrete examples of those interfaces.
- **Interfaces that allow TDM switching** – switch data depending on the time slots; the interfaces at SDH/SONET cross-connection equipment and terminal multiplexers or add-drop multiplexers.
- **Interfaces that allow switching based on LSC** (*Lambda Switch Capable*) – switch data depending on wave longitude. The example is PXC (Photonic Cross–Connect) equipment or OXC.
- **Interfaces that allow switching in space** – switch data depending on the position of data in real space. The examples are PXC and OXC that can work on single or multiple fibre level.

GMPLS problems and possible solutions

When generalized control plane which can provide communication in different network types is observed, few problems in front of GMPLS suite of protocols must be considered:

- firstly, packet switching is not the only thing. Common solution must be able to keep switching simplicity using labels for different devices working, not only in the packet area, but also in time, space (physical ports) and wavelength domain.
- secondly, not every network type is capable of giving an overall information on the content and label assignment. For e.g., packet defined networks are able to analyze packet header, check label and decide on the appropriate outgoing interface (*switching path*) which has to be used. Telecommunication equipment used in military networks (TDM, optics) is in most part very different and does not support information content analysis sent to them.
- compared to packet networks, on TDM, LSC and FSC (*Fibre Switched Capable*) interfaces can be isolated bandwidth only in discreet values. For e.g., in packet based network there could be 1, 10 or even 100 Mb/s traffic flows. However, optical network will use links which have fixed bandwidth with optical carrier OC-3 (in SDH hierarchy it is STM-1), OC-12 (STM-4) or OC-48 (STM-16). Therefore, when one PSC device initiates LSP with 10 Mb/s bandwidth, it should be propagated through optical network with fixed bandwidth – there is no much sense in isolating 622 Mb/s link for the mentioned traffic flow.

SONET/SDH networks have an important ability of fast traffic switchover from a damaged path (partially or fully) to the new one, and all this in a very short time (50 ms) [5]. This ability is very significant for potential use of GMPLS protocol in possible military integrated network.

- Appropriate control plane in GMPLS must accommodate for such a procedure and also other protection methods of granularity. Also, control plane must provide reparation of the failed paths with static or dynamic re-route process, which depends on the required class of service.
- scalability is another important issue in designing large networks, whose adaptability to change during development, aught to be quick and financially speaking feasible. Resources which are to be maintained in TDM and optical networks are much bigger than in packet based environment. It is expecting that optical networks will carry large traffic volumes on hundreds of fibres and this kind of process requires enormous effort in resolving the problems of conservation and scalability of these kinds of networks.

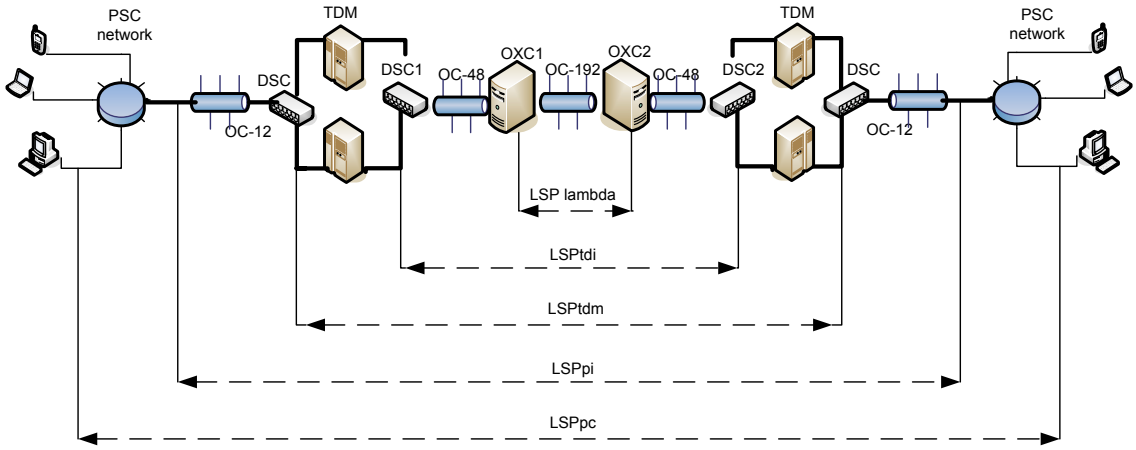


Figure 3. LSP establishing throw heterogeneous net domains

Potential use of GMPLS suite in military network structure is especially suitable from the point-view of reliability which is supported by this protocol and also in possible protection and reparation of data traffic flow, particularly with the importance of information in various military activities nowadays.

Switching variety – generalized labels and LSP establishing

GMPLS suite of protocols brings some changes to the common format of classic label used by MPLS architecture, with the purpose of switching in different domains of traffic flow. New label format is defined as *generalized label* enabling data receiver to adjust its switching part and process information (regardless of the form information is in – packet, time slot in TDM, lambda etc.).

Generalized label can represent one wavelength, one optical fibre or even time slot in TDM as well as traditional MPLS labels for packet communication over IP based network. Label in GMPLS carries information about:

– encoding type for LSP – shows label type in communication (packet, time slot, lambda);
– switching type – device ability for switching (packets, time slots, wavelengths, physical fibre);
– user information type which is being transferred through LSP path (Ethernet, ATM, Frame Relay etc.).

Label distribution begins from higher, upstream LSR device which sends requests for labels from a lower, downstream LSR. This kind of configuration is expanded in GMPLS with the ability of the upstream LSR to suggest labels for LSPs used for communication by downstream LSR.

LSP establishing in GMPLS is very similar to its configuration in the MPLS network. Fig. 3 illustrates possible network topology and LSP establishing through heterogeneous domains:

Packet Switched Capable network (*PSC network*) is connected to the TDM based network, which is connected to on optical domain capable of carrying large traffic volumes. Establishing of LSP is observed in the first packet network (device LSR 1) as well as in the second (LSR 4). For creating LSPs in other network domains, corresponding LSP paths which are tunnelling the requested LSP must be established, which is in this case required by the packet network. This scenario can be achieved by sending *PATH/Label Request* message to the destination; the message will be transferred by LSP of lower hierarchy. For e.g., Digital Switched Capable (*DSC device*) DSC 1 device sends this kind of message to OXC 1 which creates LSP with OXC 2. Only when this LSP is created an LSP between devices DSC 1 and DSC 2 can be constructed, indicated in the picture as LSPtdi.

Message request *PATH/Label* comprises the demand for a generalized label with the LSP type (adequate layer for example) and also the type of user information. Specific parameters (like signal type, local protection, bidirectional LSPs, suggested label etc.) are also transferred by this message. Downstream node will send back the message *RESV/Label* which includes one generalized label. When this label is received by LSR initiator, LSP is going to be established with its pair by sending *RSVP/PATH* message through network domains.

Summary given in Fig. 3 contains the following sequence:

– LSP established between OXC1 and OXC2;
– LSP between DSC1 and DSC2 (LSPtdi);
– LSP between LSR2 and LSR3(LSPpi);
– finally, LSPpc established between LSR1 and LSR4.

Fig.3 also shows that LSP hierarchy concept must be introduced when considering communication between different network domains. The presented model of network hierarchy enables increasing bandwidth on each hierarchy level. This idea is based on the fact that several LSPs can be observed under only one link in, for e.g., OSPF link state base (combined of all nodes and links in the network). This kind of solution facilitates dealing with the discrete nature of bandwidth in optical networks. Namely, when an optical LSP is created, it has a certain discrete value of its bandwidth, but if the LSP is treated as a link it can be given an adequate part and a free bandwidth (especially the inherent bandwidth necessity is considered). The fact that LSPs in GMPLS based network begin and end on the same type of interface, results in the placement of FSC interfaces at the top of hierarchy, followed by LSPs on LSC interfaces, then TDM and finally PSC based interfaces.

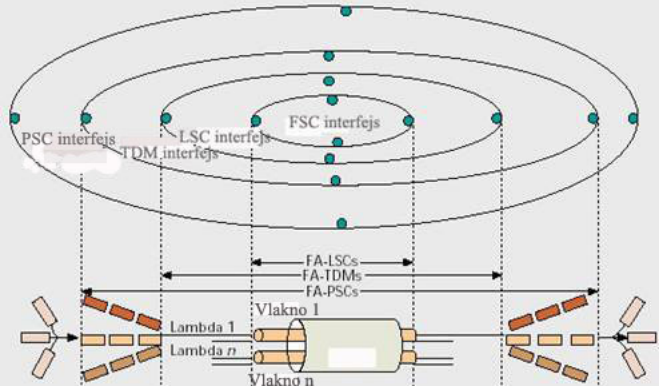
Circles, in Fig.4, represent interfaces on devices with similar possibilities. LSP of low orders are formed by high level LSPs, for example, PSC-LSP is tunnelled through

TDM-LSP and then through LSC-LSP etc. Of course, at the opposite end they are demultiplexed properly.

Configuration problems in GMPLS network

One established LSP, starting from the access network, could demand for some other LSPs in its end-to-end communication. The intermediary LSPs can be configured on TDM or LSC devices for example. All the equipment has a different character, so GMPLS must adjust to it and try to accelerate the process of making the LSPs. To solve this problem, some new methods have been introduced in GMPLS architecture: *suggested label* and *bidirectional LSP*.

Suggested label – plays a significant role in speeding the hardware configuration process towards a corresponding label. Namely, an upstream node can suggest a label to the downstream node and so, without further ado, configure its hardware towards the accepted label. However, the downstream node can reject the proposed label and suggest its own, in which case the upstream node must accept the new label. Hardware configuration operation is crucial for systems which require time for programming their switching block.



LSP's multiplexingLSP's demultiplexing

Figure 4. LSP paths hierarchy

Bidirectional LSP – is one of the solutions for protecting links in a network. LSPs in a network should be protected by establishing a pair of unidirectional LSPs, where one will protect the other. This kind of bidirectional LSPs must have the same demands of the traffic management and restoration process. GMPLS supports establishing bidirectional LSPs via a set of signalling protocol messages (*RSVP*/*PATH* and *RESV*). This procedure helps avoid signalling messages, establishes new extra paths and delays communications in a network.

Link bundling is another new feature supported by the GMPLS. This concept should provide better scaling of the network and avoid a large size for the link database. Link bundling allows the mapping of several links into one and advertising that into the routing protocol (for example OSPF or IS-IS (*Intermediate System to Intermediate System*)). This method greatly lowers the size of the link-state database and the number of links that need to be advertised. A bundled link needs only one control channel, which further helps to reduce the number of messages exchanged signalling and routing protocols.

There are some restrictions in link bundling, such as:

– all links that belong to bonded links must start and end on the same LSR pair;
– links must be of the same type (point-to-point, multipoint etc.);
– all links must have the same traffic features (bandwidth, protection type etc.);
– links must have the same switching capabilities (PSC, TDMC, LSC or FSC).

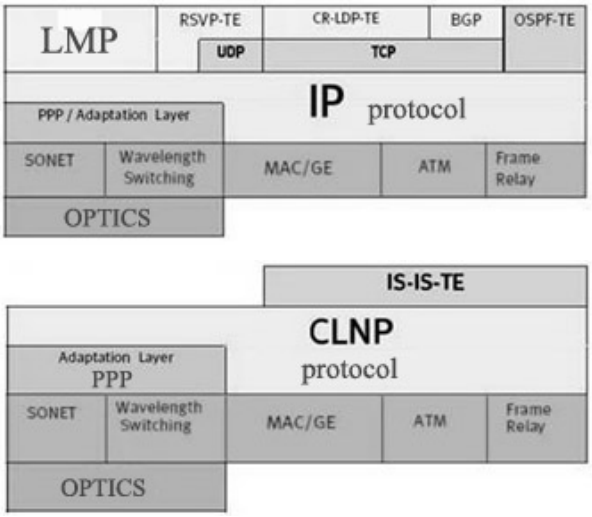


Figure 5. GMPLS set of used protocols

Bundled links result in the loss of granularity in the network resources. Nevertheless, the gain in the reduction of link-state database entries and the speed gain in table look-ups far outweigh the lost information.

GMPLS protocol suite

GMPLS is based on improvements of traffic engineering in MPLS (*MPLS-TE-MPLS Traffic Engineering*). So the fact is that protocols used in GMPLS are extended versions of the existing ones. Namely, signalling protocols are RSVP-TE *(Resource Reservation Protocol – Traffic Engineering)*, with the use of CR-LDP (*Constraint based Routing – Label Distribution Protocol*) also, and routing protocols OSPF-TE *(OSPF – Traffic Engineering)* and IS-IS-TE *(IS-IS-Traffic Engineering)*. Extensions which are introduced match the requirements needed by TDM and optical networks.

Depending on the routing protocol GMPLS uses different protocols on OSI (*Open System Interconnection*) network layer model, which is shown in Fig.5.

Greatest addition to the GMPLS suite of protocols is certainly a new signalling protocol for link maintenance LMP (*Link Management Protocol*), establishing, tearing and maintaining links between two adjacent GMPLS based nodes. This protocol manages control and data plane states between two nodes.

LMP is an IP based protocol which includes extensions of signalling protocols RSVP-TE and CR-LDP. LMP protocol defines forwarding-adjacency between nodes in the GMPLS network and determines the resources required for the links. Links may have addresses and are joined to available interfaces; also, they have some attributes (coding type, switching capabilities, bandwidth, etc.).

Most important LMP protocol functions are:

– control channel upholding in charge of negotiations about link parameters (*keep-alive* messages) and link state security;

– link connectivity verification – improves physical connectivity of links by sending *PING* test message;
– link features correlation – identification of adjacent node link properties;
– error isolation – isolating one or more errors which may occur in the optical domain.

Reliability issue

Networks with GMPLS based architecture host great efficiency solutions for the issue of reliability. A suite of protocols which are used by GMPLS has the ability to dynamically resolve errors in network operations. Guarding against drop links is ensured (*span protection*) and also end-to-end link protection (*path protection*). Mentioned protection types are illustrated in Fig.6.

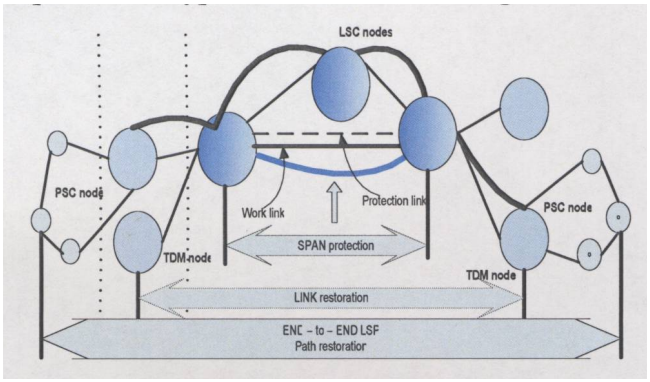


Figure 6. SPAN and PATH protection types

A fault in one type of network must be isolated and resolved separately from other networks. This is a very important feature for end-to-end LSPs that are tunnelled in other LSPs that require higher degrees of reliability, along with the hierarchy.

A common control plane that spans dissimilar networks must be able to address the varying degrees of reliability requirements within each network span.

Steps for GMPLS error restoration are very well defined:
– *detection* – new error is kept at nearest layer (example, LoL – *Loss of Light*);
– *localization* – determining the place where the error occurred and performing LMP „*handshake*“ process (*channel fail* and *channel fail ACK* messages);
– *notification* – nodes responsible for restoration are noticed with LMP protocol, meanwhile RSVP-TE informs non-adjacent nodes about LSP fail;
– *resolution* – fast switchover on previously defined LSP (50 ms) or dynamical new LSP establishing (*restoration*).

VPN – efficient solution for military environment

A well-designed VPN (*Virtual Private Network*) can provide great benefits for the military organization. It can extend geographic connectivity and improve security where data lines have not been ciphered. VPN can also reduce operational costs unlike traditional WAN and reduce transit time and transportation costs for remote military units. Using VPN can provide global networking opportunities and telecommuter support and provide broadband networking compatibility. VPNs also show a good economy of scale. Here, the MPLS solution of VPN which is an improved version of an older *overlay* and *peer-to-peer* model is considered.

Security is an important aspect of all networks, MPLS and GMPLS based networks being no exception.

There are two types of attacks on MPLS/GMPLS networks [6]:
– *Attacks on the Control Plane* – this category comprises attacks on the control structures operated by the service provider with MPLS/GMPLS cores.
– *Attacks on the Data Plane* – this category comprises attacks on the provider or end user's data.

Defensive Techniques for MPLS/GMPLS networks include:
– cryptographic techniques;
– authentication;
– use of isolated infrastructure.

One of the possible solution to improve successful and secure information transfer through military communications is using Virtual Private Network based on (G)MPLS.

The VPN is a network implemented using a shared network infrastructure but so as to provide the security and privacy of a private leased-line network. VPN has come to refer to IPSec (*IP security*) tunnels over the Internet more often, or perhaps PPTP (*Point-to-Point Tunnelling Protocol*) or L2TP (*Layer 2 Tunnelling Protocol*) dial VPN connectivity across a shared internetwork.

For the purposes of this paper, the VPNs will be IP networks where the WAN *(Wide Area Network)* core of a military network has been outsourced to a Service Provider. The IP VPN connectivity is provided across a shared IP network belonging to the Service Provider. It will turn out the BGP and MPLS-based VPNs powerful enough to provide secure connectivity (and relatively simple configuration) for both intranets and extranets.
Terminology:
– Intranet -- VPN interconnecting military headquarters site
– Extranet -- VPN connecting military units or units to external military users or suppliers. The Internet is the ultimate insecure Extranet VPN.
– Customer Edge (CE) router -- a router at a customer site that connects to the Service Provider (via one or more Provider Edge routers)
– Provider Edge (PE) router -- a router in the Service Provider network to which Customer Edge Routers connect
– Provider Core (Core) router -- a router in the Service Provider network interconnecting Provider Edge routers but, generally, not itself a Provider Edge Router
– Entry and Exit PE routers -- the PE routers by which a packet enters and exits the Service Provider network.

Virtual private networks can be a cost-effective and secure way for providing military users access to the secured networks and remote networks to communicate with each other across the Internet. VPN connections are more cost-effective than dedicated private lines – usually a VPN involves two parts: the protected or "inside" network, which provides physical and administrative security to protect the transmission and a less trustworthy, "outside" network or segment (usually through the Internet).

While the VPN connection is active, all access outside the secure network must pass through the same firewall as if the user were physically connected to the inside of the secured network. This reduces the risk that an attacker might gain access to the secured network by attacking the VPN user's host machine through other computers on the public internet; it is as though the machine running the VPN user simply does not exist. Such security is important because other local

network computers on which the user computer is operating may not be trusted, either completely or partially.

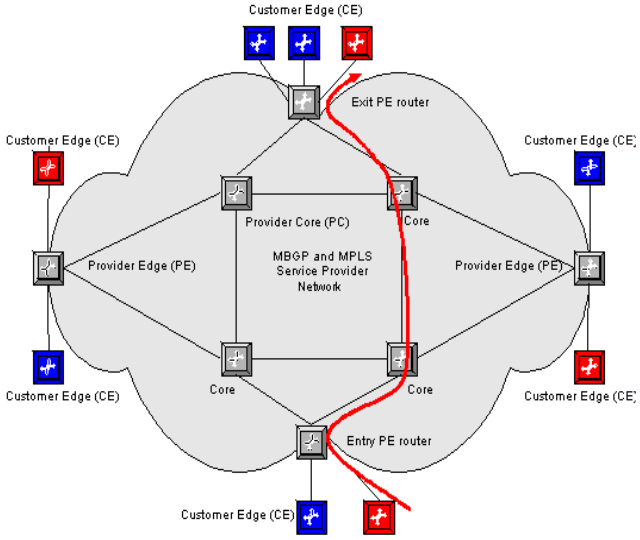


Figure 7. MPLS based VPN

Secure VPNs use cryptographic tunnelling protocols to provide the intended confidentiality (blocking snooping and thus packet sniffing), sender authentication (blocking identity spoofing), and message integrity (blocking message alteration) to achieve privacy. When properly chosen, implemented and used, such techniques can provide secure communications over insecure networks. This has been the intended purpose for VPN for some years.

Secure VPN protocols include the following:

– IP sec – commonly used over IPv4 and an obligatory part of IPv6.
– Open VPN – an open standard VPN. Users and servers are available for all major operating systems.
– PPTP, developed jointly by a number of companies, including Microsoft.
– L2TP, which includes work by both Microsoft and Cisco.

Trusted VPNs do not use cryptographic tunnelling and instead rely on the security of a single provider's network to protect the traffic. In a sense, these are an elaboration of traditional network and system administration work.

Therefore, major VPN GMPLS advantage over the common traditional packet communication is in its simplicity, since all of the routing issues are on the SP hand, not on the user part. Users on the other hand could make their own security policy and apply it in their networks.

GMPLS approach example in military communications environment

Creating a completely new military integrated communication system in the whole country is not feasible. To begin with, because of the existing infrastructure, overall functional systems and finally, because it is not financially justifiable.

GMPLS structure protocol, which would mainly rely on the part of the existing communication system, could provide fast and safe information transfer from the source to the user via various switching domains.

An example of a possible solution of how GMPLS can be applied and integrated into the military communication system is shown in Fig. 8.

From every part of the territory towards the main communication hubs, various transfer systems (radio-relay, optical) SDH, TDM, DWDM multiplex signals converge.

There are no set coaxial fibres and optical connecting cables in the Eastern part of Serbia (because of the terrain), so radio-relay communication is the only way of communication. In that part, radio-relay line is set for transferring digital channels. In the Western part of Serbia, SDH signal is transmitted by radio-relay links to larger cities and further transfer to Belgrade is ensured using optical lines. Similar radio-relay transfer system is applied in the Northern Serbia, while in the South the branchy optical network is present.

There are two solutions for the network core. One is to have a separate military core which is tremendously expensive or to rely on the national communication provider for VPN core (all routing and switching will be there). On military users' side, adequate security appliances must be provided and monitored.

Figure 8. GMPLS application on heterogeneous networks

Appropriate cabling infrastructure must also be present. This is the network part which must follow modern solutions (optical fibres and DWDM technology) for the best performance.

Conclusion

Military commanding information system must be equipped for real time communication and following that idea it is necessary to complete adequate modernization processes in these kinds of networks.

As stated in this paper, GMPLS set of protocols is a possible solution for the next generation fixed telecommunication networks based on optical and radio-relay transport systems of multiplexed SDH and SONET signals. Advantages of using GMPLS are numerous compared to the first solutions in the IP switching area (primarily MPLS). For e.g.:

– basic MPLS idea is expanded adding links where the label can be either time slot, or wavelength, or position in real space (fibre etc.);
– LSP must begin and end on the same types of interfaces;
– user traffic type is also expanded due to the fact that GMPLS can propagate SONET/SDH, 1 or 10 Gb Ethernet, etc.;

– using LSPs based on forwarding-adjacency, bandwidth utilization can be improved in cases when determining can be done only in discrete values;
– while traditional LSPs are unidirectional, GMPLS supports bidirectional LSP paths feature;
– GMPLS supports LSP destination ending on a selected port (port selection);
– with RSVP-TE fast notification, of certain network faults is supported;

Naturally, the given solution is just one of the possibilities. There is still much to be done in the area of communication over heterogeneous networks with IP traffic switching. There is a lot of space to continue the research in this area, especially concerning reliability and restoration issues, if global multimedia IP subsystems and communication in real time are to be considered seriously. Furthermore, two new and highly promising technologies are emerging – optical packet switching and optical burst switching. With this in mind, it is obvious that the research area is continuously moving throughout the optical domains, which will enable improving network operations significantly.

References

[1] LAZAREVIC,M.: *Oganizacija sistema veza u državnoj zajednici Srbija i Crna Gora*, Beograd 2006.

[2] *International Engineering Consortium*, Multiprotocol Label Switching (MPLS), On-Line Education, www.iec.org

[3] http://www.cisko.com

[4] MANNIE,E.Ed.: *Generalized Multiprotocol Label Switching Architecture,* RFC 3945, October 2004.

[5] BANERJEE,A., DRAKE,J., LANG,J.P., TURNER,B.: *Calient NetworksKireeti Kompella, Juniper NetworksYakov Rekhter, Cisco Systems - Generalized Multiprotocol Label Switching: An Overview of Routing and Management Enhancements*, IEEE Comunications Magazine, January 2001.

[6] FANG,L., CALLON,R., Le ROUX,J.L., ZHANG,R., KNIGHT,P.: *Security Framework for MPLS and GMPLS Networks*, February 2007.

[7] http://www.netcraftsmen.net

Received: 03.07.2006.

GMPLS – sledeća generacija rešenja IP komutacija

Činjenica je da je WDM tehnologija određena kao pogodan kandidat za buduća mrežna okruženja zahvaljujući svom potencijalu da zadovolji sve strože zahteve za većim propusnim opsegom i manjim kašnjenjem. Takođe, primenjene mrežne tehnologije današnjice se u velikoj meri razlikuju (heterogene su) i rešenje za komunikaciju u ovakvim okolnostima mora biti u mogućnosti da ispuni specifične zahteve. Ovaj rad razmatra GMPLS kao moguće rešenje tog problema i predlaže rešenje za specifično vojno okruženje gde ovaj set protokola može da reši problem različitih mreža i tipova uređaja. Raznovrsnost i složenost upravljanja ovim uređajima su glavni vodeći faktori u razvoju i poboljšanju MPLS skupa protokola kako bi se obezbedila kontrola ne samo domena baziranih na paketima, već i vremenu, talasnoj dužini i prostornih domena.

Ključne reči: **telekomunikacioni sistem, vojne telekomunikacije, internet protokol, generalizovana komutacija multiprotokolske labele, rutiranje, signalizacija.**

ГМПЛС - следующая генерация решений коммутации в неоднородном военном сетевом графике (сети)

Очевидно, что ЫДМ технология организации сети определена подходящим набором для будущей конфигурации сети благодаря ее возможностям удовлетворить все более строгим требованиям большей полосы рабочих частот канала связи и меньшей временной задержки. Тоже, примененые технологи организации сети в современности в большей степени различны (неоднородны) и решение для коммуникации в таких условиях должно выполнить все специфические требования. В настоящей работе рассматривается ГМПЛС в роли возможного решения этой проблемы и предлагается решение для специфического военного сетевого графика, где этот набор протоколов может решить проблему несколько различных сетей и типов устройств. Разновременность и сложность управления этими устройствами главные ведущие показатели в развитии и в совершенствовании МПЛС набора протоколов в обеспечении контроля не только областей определенных пакетами, но и временных интервалов, доменов волновой длины и доменов пространства.

Ключевые слова: **система дистанционной связи, военная дистанционная передача данных, обеспечение межсетевого протокола, обобщенная коммутация многочисленных протоколов маркировочных знаков, выбор маршрута.**

GMPLS – la prochaine génération de la solution de commutation dans l'environnement des réseaux militaires hétérogènes

Grâce à son potentiel de répondre aux exigences pour une plus grande portée et un plus petit retard, la technologie WDM est indiquée comme le candidat adéquat pour les environnements des futurs réseaux. Les technologies des réseaux en usage actuel sont très diverses (elles sont hétérogènes) et pour communiquer dans telles circonstances il faut trouver une solution capable de satisfaire les exigences spécifiques. Ce papier examine GMPLS comme la solution possible de ce problème et la propose pour l'environnement militaire où cet ensemble de protocole peut résoudre le problème de divers réseaux et installations. La diversité et la complexité de commande chez ces installations sont facteurs principaux dans le développement et la mise au point de l'ensemble du protocole GMPLS pour assurer non seulement le contrôle des domaines basés sur les paquets mais aussi ceux basés sur le temps, longueur d'ondes et domaines d'espace.

Mots clés: **système de télécommunication, télécommunications militaires, protocole Internet, commutation généralisée de marque multiprotocole, routage.**