International Journal on New Computer Architectures and Their Applications (IJNCAA) 2(1): 113-126
The Society of Digital Information and Wireless Communications, 2012 (ISSN: 2220-9085)

Infrastructure Sharing: A Cost Effective Alternative for Resiliency in 4G-LTE Mobile Networks

VENMANI Daniel Philip[*], Yvon GOURHANT[*], Djamal ZEGHLACHE[†]
[*]Orange Labs, France Telecom R&D, Lannion, France
[†]TELECOM & Management SudParis, Evry, France
email :{danielphilip.venmani, gourhant.yvon}@orange-ftgroup.com, zeghlache.djamal@it-sudparis.eu

ABSTRACT

With the fast growth of Internet and a new widespread interest in broadband networks, the unparalleled potential of Multi-Protocol Label Switching (MPLS) is leading to further research and development efforts. One of those areas of research is Path Protection Mechanism. An aim of our ongoing research is to take pragmatic approach to the "last mile" issue and provide a solution to improve resiliency primarily for 4G-LTE mobile networks by infrastructure sharing by making use of this mechanism between operators' backhaul networks. Most previous research on multiprotocol label switching (MPLS)/generalized MPLS (GMPLS) recovery management has focused on efficient routing or signaling methods from single failures. However, in this paper, we present a strategy by means of infrastructure sharing between operators considering sharing the backhaul network infrastructure to improve resiliency among the operators. The paper discusses about the resiliency mechanisms that are adapted in the backhaul network of the operators and henceforth concludes that despite the resiliency mechanisms, there are occasions when the network resources are not available for the end users which necessitates the need for sharing another operator’s backhaul, thus decreasing the overall unavailability time. This innovative solution offers significant advantages including fast recovery across multiple operators.

KEYWORDS

Backhaul Networks, Infrastructure Sharing, 4G-LTE, MPLS Modeling, Resiliency Mechanisms.

1 INTRODUCTION

Mobile Network operators have been adapting to a classical approach such as to have an exclusive use of the wireless network resources such as spectrum, sites, transmission lines, backhaul network infrastructure, core networks, etc [1]. However, cell site sharing which was mostly due to the lack of site locations and environmental aspects has been widely adopted as form of passive sharing especially in rural areas. Recent developments show further expansion towards the concept of ‘resource sharing’ i.e. wider network infrastructure sharing and, as expected, spectrum sharing. Active sharing (e.g., Radio Access Network (RAN) sharing but not limited to this) has been already set up by operators in different ways (mostly in Europe due to the ease of political and regulatory issues) which includes 3G RAN sharing between T-Mobile & Hutchison 3 UK, Vodafone & Hutchison 3 Sweden, Orange & Vodafone Spain. It is considered seriously for the 3G deployments even in urban areas such as the small towns in Spain with a population range of 1000 and 25000 people, since it achieves, in addition to the passive sharing, roughly 43% saving in Capital Expenditure (CAPEX) and 49% in Operating Expenditure (OPEX) [2]. Besides, infrastructure sharing has a good impact on energy consumption which is primordial in emerging countries. Africa as a whole is characterized by a very low penetration rate of fixed networks (e.g. 0.7% in Senegal, 3% in Cameroon). By contrast, a significant and rising part of the population owns a mobile phone: 25% on average [3]. Both the rurality of the population and its insolvency acts as a brake upon prospective deployment of fixed infrastructures taking into account the huge investments necessary to install wired solutions. While satellite-based access solutions (VSAT) are too expensive to be deployed widely, a growing set of alternative technologies have emerged that raise hope for ambitious broadband access roll-outs through contained capital expenditure.

Now within this context, focusing towards emerging countries where operators are newly deploying their mobile network infrastructure, enhancing reach through the creation of infrastructure is the need of the hour. To maintain increased growth levels, the service providers need to push out to rural and remote areas. However, the capital costs for this are very formidable and are simply not addressable through the revenues currently generated. The ever falling tariffs and the resultant decline in Average Revenue Per User (ARPU) has become a serious area of concern for service providers in emerging countries. Declining ARPU leaves the service provider with lesser amount of re-investible funds for expansion of service, which otherwise could have been far more widespread by now. Hence, it is becoming an accepted practice for operators to share site locations and masts. There are also examples of sharing complete network operations. In emerging countries such as the sub-Saharan African countries like Kenya, Uganda, Nigeria etc. as well as the Eastern European countries, where the backhaul network connectivity is mostly based on microwave, it is undesirable for each cellular operator even if they were able to afford it, to replicate expensive telecom infrastructure to reach the subscribers in remote rural areas. Hence, they go for access network sharing where the same e-Node B is shared between operators.

Our solution is based on infrastructure sharing between operators where the backhaul networks of the operators is shared. The sharing scenarios are defined for two situations. The first one, at times where there is a failure in one of the sharing operators' networks and the second one is at times where there is the traffic peak condition encountered. This allows mobile network operators to leverage on existing infrastructure to provide affordable and reliable services to urban as well as rural and remote consumers, especially to support the increasing data traffic due to broadband services. Infrastructure sharing is nevertheless equally important in the urban areas where the presence of 2 or 3 operators and a rapidly increasing mobile subscriber base for data and broadband services, is resulting in more and more investments for infrastructures being put up by each operator to cater to higher traffic requirements. This ultimately leads to the need for additional backhaul links. Traditionally backhaul networks have been acquainted with Ethernet cables, fiber, copper wires, microwave and other means of limited and expensive cabled infrastructures - each with its own advantages and disadvantages. Apart from sharing the equipments to reduce cost between operators and increasing coverage for customers, we define infrastructure sharing to be exploited to the next level of using it for resiliency purpose in which the backhaul network of the operators are shared. Our current proposed solution takes into account infrastructure sharing between microwave backhaul connectivity only taking into account the huge investments necessary to install wired solutions in emerging countries. Thus in this paper, the concept of backhaul network infrastructure sharing among the operators during peak traffic conditions or network failure situations is provided as an alternative for resiliency mechanisms. Current resiliency mechanisms are based on over-dimensioning and rerouting mechanisms that are mainly deployed on core networks but they cost too much for being largely deployed till the last-mile backhaul network compared to the probability of outage. Our solution paves a way for seamless connectivity even till the last mile without additional links. In order to provide a low cost alternative, the basic consideration for our solution requires prerequisites that do not exist today in LTE e-Node B implementations. Typically e-Node B should have atleast minimal IP support, which gives the ability to route the traffic via another operator backhaul network. With our solution, e-Node Bs are expected to behave as Provider Edge routers with minimal IP capabilities or a routing node, with full

IP capabilities. In addition to having the basic IP capabilities, the operators also must agree upon the resource allocation in the Service Level Agreements (SLAs) clearly. Hence, in this paper, the state of the art dealing with the problem characterization associated with the set backs of the existing routing protocols and the use of resiliency mechanisms already adapted by the operators in order to backup their networks is clearly detailed.

The rest of the paper is structured as follows. Section II describes the problem characterization comprising the network availability problems, protection and restoration mechanisms and finally detailing about the backhaul architecture of mobile networks. This is followed by section III, where we have described resiliency by means of infrastructure sharing. Section IV presents our simulation results presenting the advantages of MPLS recovery over the existing recovery mechanisms. This is followed by the conclusion.

2 PROBLEMS CHARACTERIZATION

2.1 Network Availability

Network availability is defined as the ability of a network to deliver continuous operation without service interruption. In other words, it is the percentage of time during which the network is working properly and is able to provide services to its customers according to service level agreements (SLAs). In practical terms, it can be concluded that, the higher is the network availability, the better. Usual desired values, depending on service requirements, range from 99,99% to 99,999% (the latter is often called “five nines” and is considered the ultimate availability). Network can be impacted by failures, which cause network downtime and thus decrease the availability or increase the unavailability, usually measured in number of minutes per year during which the network is not fully available. The reliability of each network functional block (e.g. a link, a node, a linecard within a node, SFP module on a linecard, etc.) is characterized by a parameter called MTBF - Mean Time Between Failures. MTBF values for network equipment are usually provided by equipment vendors. MTBF for links can be assessed based on statistical data (e.g. the chance of a fiber cut calculated by taking into account all fiber cuts that affected a certain network in a certain period of time). When a failure occurs and the network becomes unavailable, a repair action is required to bring the network back to a fully functional state. The repair process takes some time, during which the network remains unavailable. Depending on the type of the failed functional block, repair times may vary (e.g. a fiber cut is much more difficult to repair than a failed linecard). Therefore, each type of failure can be assigned with an MTTR (Mean Time To Repair) value, based e.g. on statistics gathered during the actual network operation. Availability of a network segment or a whole network can be evaluated using different models, which usually take into account MTBF and MTTR of each functional block in the network. If the results of such analysis are not satisfactory, the availability of the network can be increased by using automated recovery mechanisms. Such mechanisms allow for quick network failover, so they decrease the network repair time and increase its availability. The table below points out some standard MTTR based on French Networks.

Table 1. List of MTTR for hardware and infrastructure

Elements	MTTR (in hours)
Optical fibre/ Copper Cable	14
ODF/CDF	2
DU/Node B	6
Hardware/ IDU	4

They are dependent of the maintenance logistics applied to the local network context conditions (geography, location of the spares) and can vary in function of the local network context specificities, consequently. Moreover, MTTR for urban and rural area can be also dissociated. As a matter of fact, every operator establishes their own set of different resiliency mechanism at every relevant layer (namely datalink, transport, logical IP) of the network to protect the network from failures. An important concept used to describe automated recovery mechanisms is the recovery cycle. It describes the phases of a recovery process and timing associated with those phases. A generic network recovery cycle is shown in fig. 1 below.

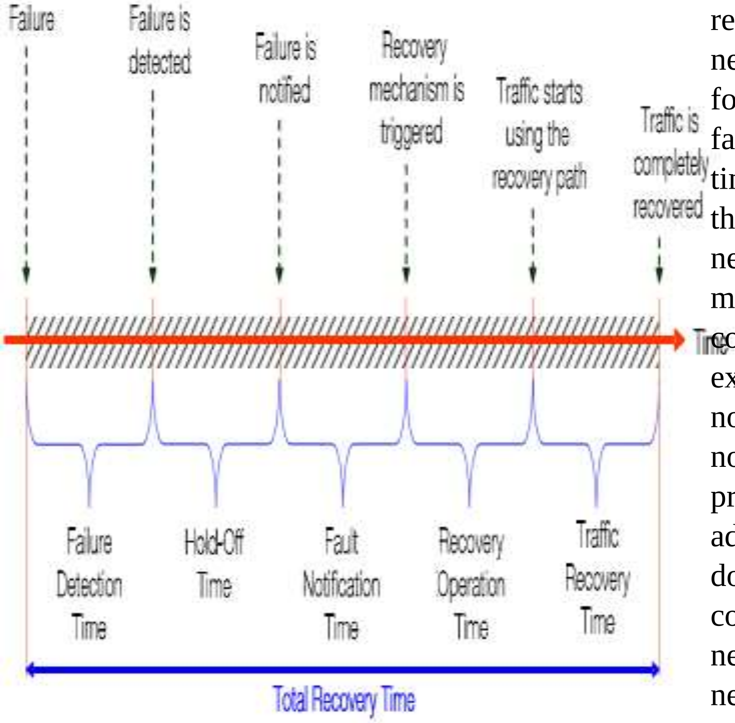

Figure 1. Generic Network Recovery Cycle

If a failure in the network occurs, it could take some time before a node adjacent to the failure detects the fault. This time may depend on the speed of fault detection in a lower communication layer and the speed of notification of this fault toward upper layers. Once the fault is detected, the node that detected the fault may (or may not) wait some time before it starts sending notification messages toward the other nodes in the network. For instance, this hold-off time could allow a lower layer recovery mechanism to repair the fault. As soon as the fault notification message reaches the node responsible for performing the recovery operation, the recovery mechanism is triggered. Usually some time is necessary until the last recovery action finishes and the traffic can start to flow over the recovery path. This time is referred to as recovery operation time (not to be confused with the total recovery time). For example, this time can include the exchange of messages between the different nodes involved in the recovery action to coordinate the operation. After the recovery operation finishes, it can take some time until the traffic reaches its destination over the recovery path. This traffic recovery time may depend e.g. on the propagation delay along the recovery path or the location of the fault within a network. All time spans mentioned above account for the total recovery time that passes between a failure and full traffic recovery. The total recovery time may vary depending on different factors, like the recovery mechanism used the topology of the network (in case of segment or network-wide mechanisms), etc. For a given mechanism some components of the recovery time may be zero. For example, if the node that detects the fault is the node responsible for repair action, the fault notification time is negligible. However, all of these prove that the existing resiliency mechanisms adapted by operators still prove to have their own downtimes and hence this led to the primary consideration to propose to share the backhaul network infrastructure with other operators under network failure conditions. The availability of the network can be increased by sharing or using the backhaul network infrastructure of the other operator with whom the sharing policy is concluded. Such mechanisms allow for quick network failover.

2.2 Protection and Restoration

In general, recovery mechanisms can be divided into two main categories: protection mechanisms and restoration mechanisms. The difference between those two is in the way the resources used for traffic recovery are allocated. With protection mechanisms the recovery path is calculated and signaled (or configured) before the failure. Restoration mechanisms do not have any pre-signaled or pre-provisioned recovery resources prior to the failure, so they have to set up the recovery path after the failure occurs. This difference is reflected in the total recovery time of protection and restoration mechanisms. In case of protection mechanisms the recovery operation time is minimized (sometimes even negligible), whereas in case of restoration mechanisms it can be a significant component of the total recovery time, especially with network-wide recovery mechanisms in larger networks. The drawback of protection mechanisms is that they may require a significant amount of network resources (control plane resources, such as established PWs or LSPs, and forwarding plane resources, i.e. the actual use of network bandwidth) for the recovery purposes. Another disadvantage of protection mechanisms is their lower flexibility – restoration mechanisms can dynamically react to any failure in the network.

2.3 Recovery in Mobile Backhaul Networks

A mobile backhaul network transports several different types of traffic flows. They are User Plane, Control Plane and Management Plane. Each type of flow has different requirements in terms of bandwidth, packet loss rate, maximum delay, delay variation, etc., based on the mobile service carried by a particular flow. Flows also have different requirements in terms of High availability (HA). The HA requirements (e.g. the maximum service unavailability in minutes per year) of each mobile service are evaluated based on the impact of network failures and their duration on the service (i.e. service interruption time), mainly from the user experience perspective. If the results of unavailability analysis performed on the network show that high availability requirements of a certain service (or services) are not met, recovery mechanisms can be implemented to protect the traffic flows carrying those sensitive services. Recovery mechanisms working in lower layers (physical layer or data link layer) usually protect all traffic flows carried by the protected resource. In higher layers however it may be possible to implement recovery mechanisms only for a particular type of traffic flow, while leaving the less sensitive traffic unprotected. This can reduce the amount of backup resources (control plane and/or forwarding plane) required in the network if protection mechanisms are used (as opposed to restoration mechanisms.

2.4 Recovery Domains

In order to properly discuss recovery mechanisms in mobile backhaul networks, we have defined several recovery domains. They are shown in fig. 2 below.

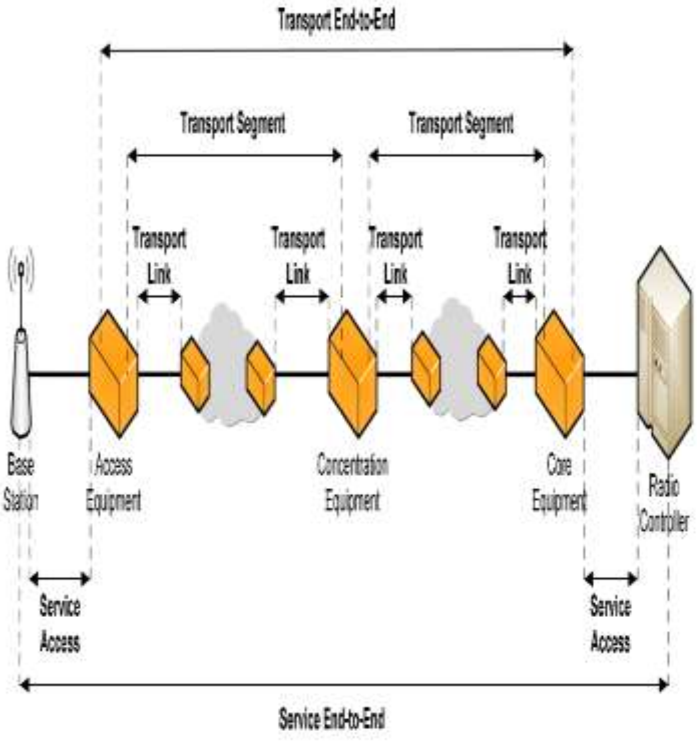

Figure 2. Recovery Domains in Mobile Backhaul Network

Recovery domains can map both to physical segments of the network (e.g. single link, L2 segment, etc.) and to operational segments (parts of the network managed by a single operational team). The main distinction is made between two operational network domains, usually managed by different teams, especially in larger mobile networks: Service (RAN) and Transport. The Service domain covers all recovery mechanisms that involve the RAN equipment, whereas the Transport domain covers recovery mechanisms working within the mobile backhaul network. Service domain is further divided into two sub-domains. The Service Access where connection between

RAN equipment and transport equipment is established and the Service End-to-End where end-to-end traffic flows carrying mobile services between RAN nodes. Transport domain is further divided into three sub-domains. The Transport Link where single physical link is established between two transport nodes (e.g. optical GE link between CSG and MASG). The Transport Segment where a segment is established within the transport network (e.g. MASGs in the Middle Mile network interconnected with SDH MW or an EMS cloud between base station and PoC). The Transport End-to-End where an end-to-end path through the transport network is established (between transport equipment at the cell site and transport equipment at the RNC site). Recovery mechanisms working in adjacent network segments can co-operate in order to provide end-to-end recovery capabilities. This cooperation can be performed within the same recovery domain (e.g. two different MPLS transport layer recovery mechanisms cooperating within a single transport network) or between different domains (e.g. MPLS service layer mechanism in the transport end-to-end domain cooperating with a data-link layer mechanism working in the service access domain). We take this to further explore our solution that is based on MPLS for backhaul infrastructure sharing between operators.

3 RESILIENCY SOLUTION BASED ON INFRASTRUCTURE SHARING

Current resiliency mechanisms are based on over-dimensioning and re-routing mechanisms that are mainly deployed on core networks but they cost too much for being largely deployed till the last-mile backhaul network compared to the probability of outage. Our solution paves a way for seamless connectivity even till the last mile without additional links. In order to provide a low cost alternative, the basic consideration for our solution requires prerequisites that do not exist today in LTE e-Node B implementations. Typically e-Node B should have atleast minimal IP support, which gives the ability to route the traffic via another operator backhaul network. With our solution, e-Node Bs are expected to behave as Provider Edge routers with minimal IP capabilities or a routing node, with full IP capabilities. In addition to having the basic IP capabilities, the operators also must agree upon the resource allocation in the Service Level Agreements (SLAs) clearly. The preliminary pre-requisite for backhaul network sharing is the ability of the e-Node B to route the traffic via another operator backhaul network, thus sharing of backhaul network infrastructure. It is a non-negotiable concern that until now, there are only limited research results that show the way for dynamically routing resources between operators when they share their network. i.e. when two operators share their network including sharing their backhaul network infrastructure and when either one of the operator’s link fail, there is no mechanism that defines how the traffic density has to be re-routed via the other operators available link based on transmission metrics, yet with meaningful energy savings. Our scenarios for backhaul network sharing essentially require that the e-Node B is capable of detecting fault in a link on its own network and automatically routing the traffic towards another operator backhaul network with whom the sharing agreement is signed. To do this, the need to consider several routing protocols for the backhaul of LTE-EPC architecture arose. Therefore, it becomes self-explanatory that the choice of protocol here is either a connection–oriented or connection-less protocol. Cooperative wireless access networks [4] employing connection-less packet forwarding techniques is a burgeoning field of research. As opposed to the approach in which each terminal autonomously transmits to the access point or base station, cooperative communications assume that multiple terminals or relays collaborate to improve the overall effectiveness of the network. Cooperative access networks, when combined with appropriate coding techniques [5], can be used improve the robustness of communications thanks to the increased diversity [6], [7]. The cooperation can take different forms. It can bee among peers, such as in [8], [9], or using fixed dedicated relays [10], [11]. In both cases, it is necessary that the two devices willing to cooperate are in each other’s transmission range. If the nodes, relays and base stations belong to several different access networks (operated by different providers), the opportunities for collaboration are greatly diminished. Nevertheless, mobile operators are reluctant to base their mobile backhaul network on connection-less packet networks. The concern is that connection-less networks will not be capable of providing the levels of quality and reliability necessary to support voice services. Connection-less packet networks also demand new operational procedures and re-training of staff. Hence the dilemma facing mobile operators: the demands of future services are best met using a packet-based network, but connection-less packet networks could affect existing revenue-generating voice services. However with the introduction of connection-oriented packet networks, there is a possibility of solving this dilemma.

Therefore, in this paper, we present a migration plan using connection-oriented packet transport IP/MPLS [12] solution, which provides a path to a fully packet based network with the levels of quality and reliability that can support both existing and future services. However, it has to be noted that the routing protocol that is decided to be adapted on the backhaul network infrastructure has to be compatible with the rest of the operators who agreed to share the infrastructure, since we are dealing with protocols that has to handle network sharing scenarios, i.e. both the operators must agree upon the same protocol (IP/MPLS) to be used on their backhaul network. With 3GPPs focus towards making an all-IP architecture, enabling e-node Bs with IP capability seems to be very feasible in the near future.

From our previous conclusions, the choice of the routing protocol for the backhaul network infrastructure is decided to be IP/ MPLS. Hence, every e-Node B and every router within the backhaul architecture has to be implemented with IP/MPLS capability, thus capable of detecting the failure of delivery of packets by Time to Leave (TTL) value defined in the MPLS packet format and thereby forwarding the packets to the adjacent e-Node B of another operator. Here, the e-Node B does not choose to forward the packet to another neighboring e-Node B of its own operator. This is to minimize and avoid the peer-to-peer links between e-Node Bs of the same operator and thus reducing the number of additional links for resiliency. This is depicted in fig. 3 and fig. 4 that represents a scenario when the last-mile link in operator A fails.

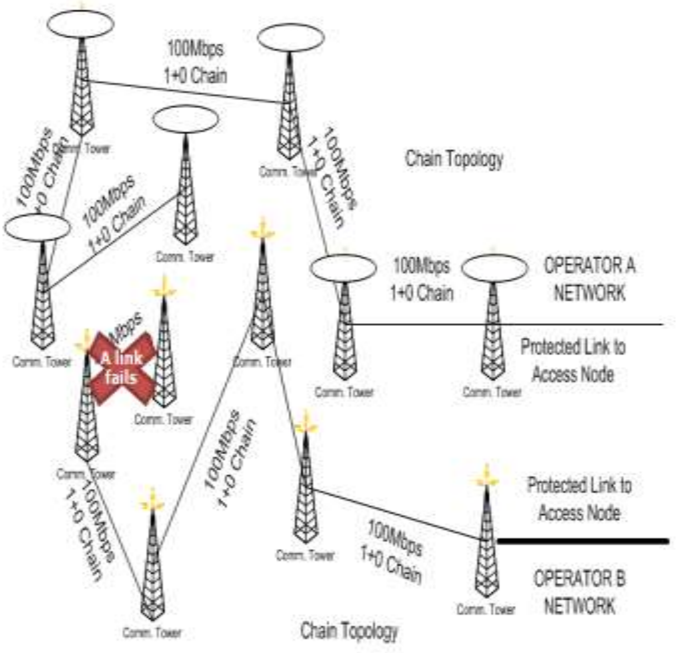

Figure 3. Link Failure in Operator B last mile backhaul network which is a chain topology by default

Thus, the operators who agree to share the network infrastructure must also agree upon deploying the same routing protocol, i.e. IP/MPLS in their networks.

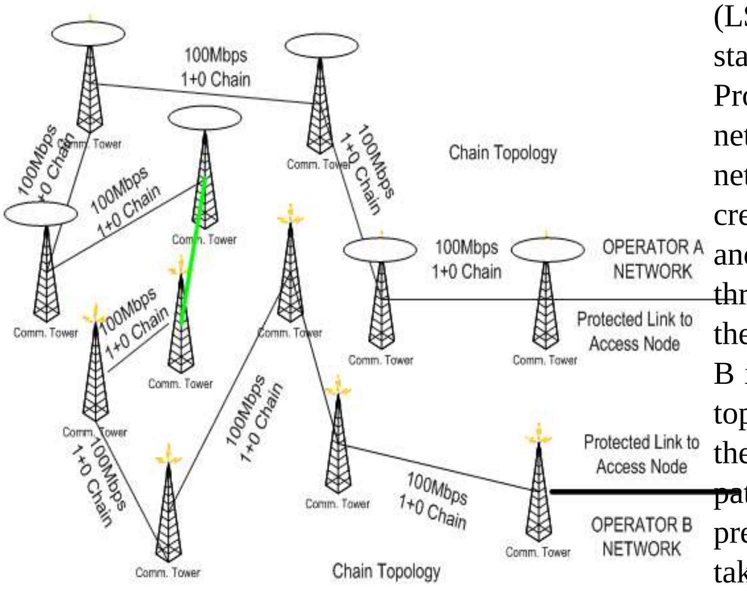

Figure 4. Backhaul Network sharing between operators resulting in a ring topology (Thanks to e-Node B's forwarding capability)

As per the LTE network architecture specification [13], the e-Node B establishes S1 and X2 interfaces. The S1 interface terminates on the anchor point Gateway (aGW). The X2 interface runs between e-Node Bs and is used for neighbor discovery, handovers and cell optimization. Each e-Node B needs to be able to communicate with its direct neighbors. Based on LTE ongoing standardization and implementation, the S1 and X2 interfaces will be based on IP over Ethernet [14]. Taking advantage of this IP capability, we establish the two fundamental connections in the mobile backhaul network. One is the point-to-point connection between the transport equipment connecting the cell sites and the transport equipment connecting the central sites for transporting S1. Also, S1 interface of the operator A has a point-to-point connection with the transport equipment connecting the central sites of operator B and vice versa for the other operator as a result of the backhaul network sharing agreement. The other one is the point-to-point connection between the transport equipments/interfaces connecting two e-Node Bs for transporting X2. Now incorporating IP/MPLS protocol within the backhaul network of the LTE architecture, the Label Switched Paths (LSP) and Pseudo Wire (PW) are established using static provisioning. The e-Node Bs serve as Provider Edges (PEs). LSPs are established by the network operator here in this scenario for backhaul network sharing purpose between them, such as to create network-based IP virtual private networks and also to route traffic along specified paths through the network inorder to differentiate between the operators. When a labeled packet from operator B is received by an MPLS router of operator A, the topmost label is examined. Based on the contents of the label, the packet is routed along the specified path designated for operator B. Routers can have prebuilt lookup tables that tell them which path to take based on the topmost label of the incoming packet so they can process the packet very quickly. Since the path is setup statically, it is much easier to plan the network, because at any given time, operator can view the overall network usage and based on this information can expand the network in much more predictable and efficient manner. In addition, every LSP/PW connection is bi-directional, which means both forward and return path will traverse through the same set of MPLS-TP nodes. This function is also referred to as deterministic data plane. This function allows operators to not only troubleshoot the network with confidence but also that the operators can identify the troublesome parts of the network before the actual problem really happens.

The advantages of adapting to a solution based on this scenario are

- The main advantage being that the solution is simple technically.
- The user traffic coming to e-Node B effectively utilizes the capacity on both the operators' backhaul network resource, i.e. network resource of its own backhaul and network resource of the sharing operator.
- The operators do not have to take care or even pay attention to the traffic of the sharing operator that flows through their own backhaul network infrastructure after the provisioning.
- Since, they only "share" their available bandwidth with the other operator and not really provision with any additional links, this kind of

sharing does not incur any additional cost to operators.

- The operators have the liberty to choose to prioritize the type of traffic that he would want to flow in the sharing backhaul bandwidth. Even better is, the operator can nonetheless care about the traffic priorities and just re-route a part of its own traffic in the shared bandwidth even at times when there is no failure in its own network.
- Traffic prioritization and service differentiation is not necessary (at times when there is no failure in their own network) considering this situation since the operators are given complete liberty with the additional bandwidth they are allocated by the sharing operator.

However, the drawbacks are

- Ratio needs to be defined effectively because it may be difficult to ensure contracts on quality (e.g., delay, jitter, loss rate, availability) and availability.
- An operator may pay for a backhaul network having good quality and another operator may benefit of that without needing to invest in a backhaul network having the same quality for the benefit of the other operator. But, this situation already exists in the traditional active infrastructure sharing, which is always considered a “Contract or SLA issue”
- The operators still could monitor the traffic flows of each other, if they wanted to. But, this could be forfended strictly by mentioning in the SLA.

4 SIMULATION RESULTS

4.1 MPLS Recovery

As described in the previous section, our approach for backhaul sharing under network failure conditions is based on IP/MPLS. There are several approaches for MPLS recovery. Some of them are centralized, other are distributed. The centralized approaches are known as global recovery and the distributed approaches are known as local recovery, e.g. Makam approach [15], [16], [17], [18], [19]. The main difference between the global and local recovery is determined by the way they handle the recovery of the MPLS network. When using local recovery, the recovery path selection or switching is done by the nearest to the point of failure upstream Label Switch Router or LSR. If global recovery is used, the alternative backup path selection is done by so called Protection Switch LSR or PSL. In most of the cases the implementation of the local recovery ensures fast response time in the case of link or node failure but is characterized with considerable amount of management load in order to achieve good results. The usage of the global recovery ensures that the whole path is protected thus overcoming potential link or nodes outages. This is really a very good advantage but from the other hand in order the global recovery to function correctly the PLS needs to be informed when a failure occurs. This PLS failure notification is necessary in order the PLS to start to perform its recovery actions. There are different approaches for implementing global recovery. In [20] is described a directory based approach which claims to offer fast notification of the MPLS LSP failures thus allowing good response time when switching to the backup LSPs. Some of the disadvantages of the described model are lack of tools for initial modeling and integrated simulation of the MPLS network and using non native programming technologies for extending the functionality of the existing MPLS nodes. The initial MPLS network model is created using the OPNET Modeler which is characterized with broad range of modeling functionality with full MPLS capabilities. The choice of the OPNET Modeler is determined by the fact that offers fully integrated environment for network modeling and simulation which allows for focusing on the model optimization and improvements and not on the model creation. Thus, our choice of simulation is also based on OPNET modeler for evaluate our results.

4.2 Traffic Engineering with Dynamic LSPs

Traffic engineering can be made with static or dynamic Label Switched Paths (LSPs). The goal for this scenario is to practice Traffic Engineering using dynamic LSPs. Dynamic LSPs can be set up using CR-LDP or RSVP. They can use bandwidth reservation to support traffic constraints. They differ in RSVP. RSVP sends periodic refresh messages to maintain the LSPs whereas CR-LDP does not. To find the path that LSPs will use routing protocols are used. There are two options, use IGP (Interior Gateway Protocol) or CSPF (Constrained Short Path First). If a LSP is setup using IGP you cannot do traffic engineering with dynamic LSP because constraints are not take into account. Fig. 5 is the simulated scenario. There are several conversations and the MPLS deployment was carried out using “Configure LSPs from Traffic Conversation Pairs…”. A dynamic LSP is created for every conversation pair, these LSPs are created from the ingress LER to the egress LER without any strict node between. In this way Traffic Engineering cannot be implemented because, if CSPF is used, the only effect is that the LSP cannot tear up. If the LSP cannot be tear up the traffic is forwarded using IP forwarding. So the traffic is forwarded in the same path that uses the dynamic LSP (that is because there are no strict nodes between the ingress LER and Egress LER) so congestions and delays will happen.

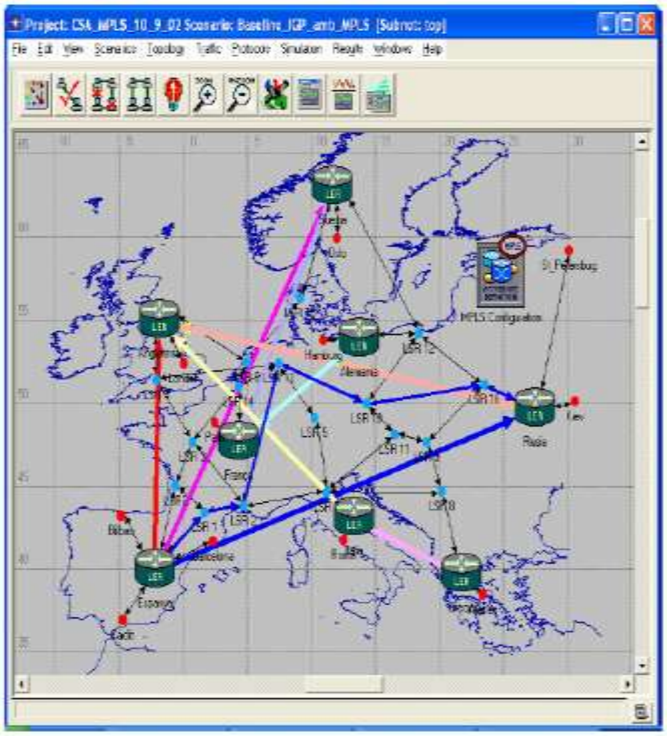
Project: CSA_MPLS_10_9_02 Scenario: Baseline_IGP_amb_MPLS [Subnet: top]
File Edit View Scenarios Topology Traffic Protocols Simulation Results Windows Help
LER
Oslo
St_Petersburg
MPLS Configuration
Hamburg
Alemania
LSR12
LSR10
LSR15
LSR11
LSR8
Kiev
Rusia
Francia
LSR2
LSR1
Bilbao
Barcelona
España
Cadiz
Italia

Figure 5. Network Topology with Dynamic LSPs

However if there isn’t congestion the forwarding paradigm using MPLS is better than the standard IP forwarding that’s shown in fig. 6.

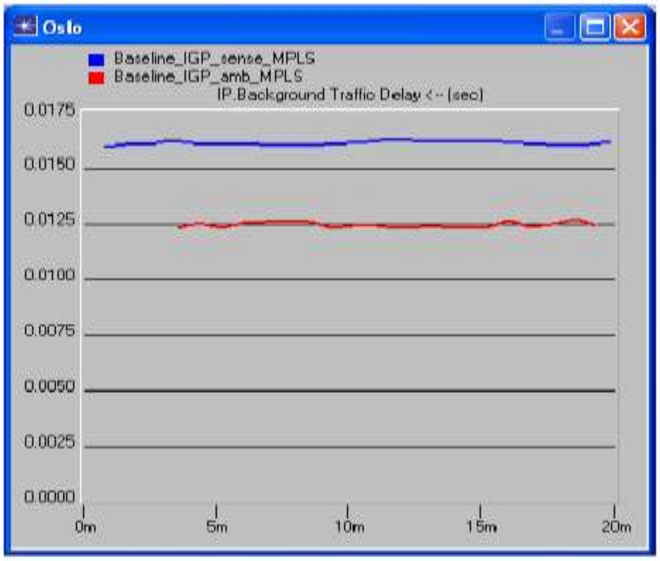

Figure 6. MPLS forwarding is faster than IP forwarding

Fig. 7 shows a LSP configured with a traffic trunk profiles that discards the traffic out of the profile. The traffic delay is better than without MPLS (but the reason is the discarding of the packets) so it is not an advantage.

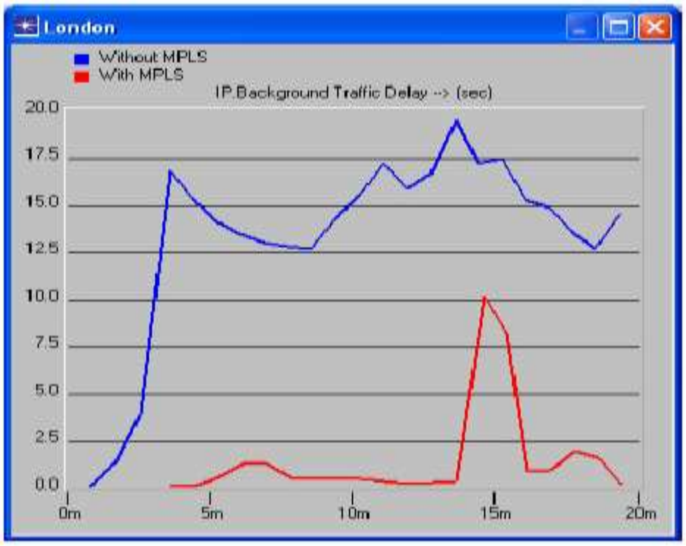

Figure 7. IP background Traffic Delay

The conclusion is that if you want to do traffic engineering you must configure some strict node and you can use OPNET simulator to view the effects of this new configuration previously to deploy in your production network.

4.2 Failure Recovery

The goal for this scenario is to demonstrate that MPLS failure recovery is very effective since our approach is based on MPLS recovery between operators who share their backhaul. This scenario will compare two protocols, RIP and MPLS, and its failure recovery response. The traffic was modeled in an event mode to obtain more accurate results. Failures were configured “randomly”, infact failures are configured in the middle of the RIP update timer. In fig. 8, it is shown the network topology without LSPs and in fig. 9, the results of simulation. In fig. 10 there are a few seconds (about 15 seconds) where no traffic is forwarded to destination, and traffic is forwarded through secondary route although the primary route is recovery until the secondary route fails.

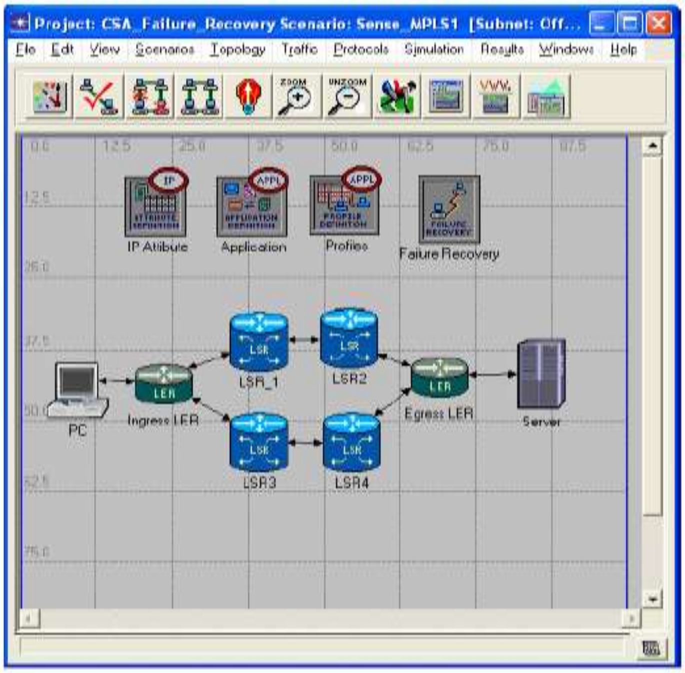

Figure 8. Failure Recovery Topology

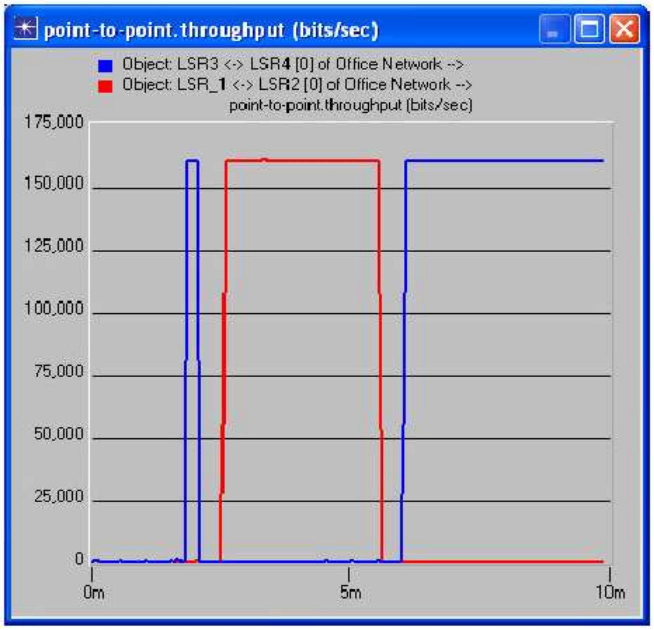

Figure 9. RIP Failure Topology

In fig. 10 is shown that recovery is done in a few millisecond and when the primary path is recovered preempt and the traffic is routed again through the primary path. When the secondary path fails, the traffic doesn’t realize it. All of this accomplish configuring a backup LSP through the secondary route, this type of protection is known as end-to-end protection. Our simulation results are restricted to only this LSP protection scheme, since in OPNET

8.0 this is the only LSP protection scheme available.

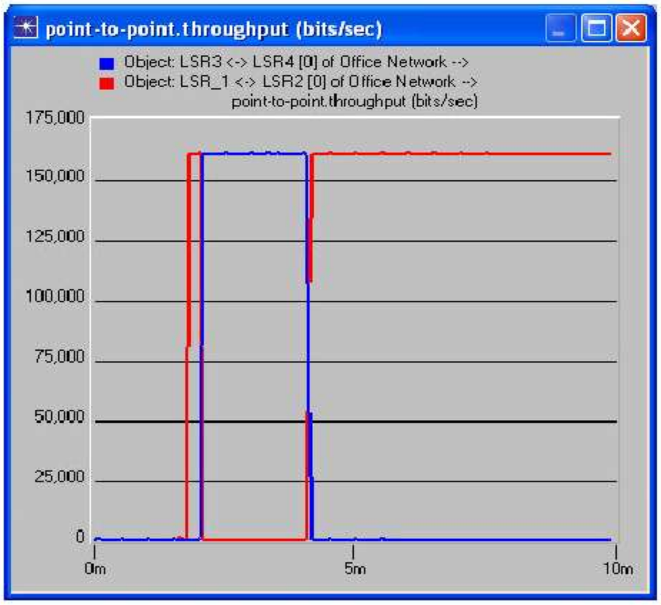

Figure 10. MPLS Failure Topology

The traffic configured was UDP because if TCP is used TCP acknowledges can be drop and traffic flow would be affected. The other effect arises when the secondary route fails. This affects the primary route because the acknowledges were routed through the secondary path. If TCP traffic is used it is recommended to meet protection in both directions. These studies shown that MPLS can offer multiples items that help to increase the performance of a network like Traffic Engineering and Failure recovery.

5 CONCLUSION

As the mobile communications sector continues its relentless expansion with more subscribers and more advanced services generating ever-greater volumes of traffic, operators must invest in their infrastructure to provide the bandwidth to meet demand. Network congestion or mobbing and traffic overloading is resource-sharing problem, which will upswing whenever resources are not enough to meet users demands. The LTE/EPC evolution is an evolution towards an all-IP architecture and will fundamentally change how mobile backhaul networks are built in the future. The availability of ethernet-enabled e-Node Bs and the evolution towards LTE/EPC pushes IP awareness further into the edge of the mobile network. Mobile operators are beginning to view these backhaul networks like carrier ethernet environments offering multiple concurrent services. In this article, we have presented a simple model for resilience, which enables various recovery mechanisms in an MPLS/GMPLS framework between operators who agree to share their backhaul networks. We have derived the conditions to test the availability of backup paths that satisfy the resilience constraint for a general mesh-type MPLS/GMPLS network with an arbitrary configuration. Simulation results show that the MPLS based recovery mechanism provides faster service recovery time and better blocking probability than the conventional rerouting mechanism of IETF standards. With all these factors leading to the consideration of maintaining QoS, which essentially has become an important aspect in the networks mostly by the increased usage of real-time communications in many production networks. The level of recovery directly affects the service level (data loss and recovery time) provided to end users in the event of a network failure. There is a correlation between the level of recovery provided and the cost to the network. The growing demand for QoS has led to significant innovations and improvements on the traditional best effort IP networks. Technologies such as MPLS provide important advantages over the classical hop-by-hop routing decision processes. The ability of MPLS to apply equally well to various layer 1 technologies, including Wave Division Multiplexing (WDM), makes this technology a strong contender for current leading edge and future networks. Furthermore, due to its label switching architecture, MPLS can provide very fast recovery mechanism complementing existing lower layer protection schemes. The development of new techniques to provide path protection at the MPLS layer will certainly continue. Simulation results show recovery times of a few milliseconds which displays the potential for this proposed solution for MPLS inter-domain protection. With backhaul network infrastructure sharing, the cost reductions will lead to a reduction of business risk for the involved operators. The cost and energy reduction in this scenario is of a similar magnitude, since more traffic can be served with the same equipment before additional sites are needed. With all these in mind, backhaul network infrastructure sharing could be one of the problem solvers to tackle the issue of restoring network failures or undermining peak traffic problems.

6 ACKNOWLEDGEMENT

The authors would like to thank Isabelle BOYER-HEARD, Christian COLLET, Pierre-Luc François, Orange Labs, France Telecom R&D, Lannion, France, for their valuable inputs towards evaluating the available resiliency mechanisms and for the MTTR values of the French network.

7 REFERENCES

1. Jorswieck, E.A., Badia, L., Fahldieck, T., Gesbert, D., Gustafsson, S., Haardt, M., Ho, K.M., Karipidis, E., Kortke, A., Larsson, E.G., Mark, H., Nawrocki, M., Piesiewicz, R., Romer, F., Schubert, M., Sykora, J., Trommelen, F., Van den Ende, B., Zorzi, M: Resource Sharing in Wireless Networks: The SAPHYRE Approach. In: Future Network and Mobile Summit 2010 Conference Proceedings, Cunningham, P. and Cunningham, M (Eds), IIMC International Information Management Corporation, 2010, ISBN: 978-1-905824-16-8.
2. Frisanco, T., Tafertshofer, P., Lurin, P., Ang, R.: Infrastructure Sharing for Mobile Network Operators From a Deployment and Operations View. In: Network IEEE Operations and Management Symposium, 2008, NOMS 2008.
3. Digital World Forum, Low cost broadband access and infrastructure, http://digitalworld.ercim.eu/wp3.html.
4. Battiti, R., Cigno, R., Sabel, M., Orava, F., Pehrson, B.: Wireless LANs: From War Chalking to Open Access Networks. In: Mobile Networks and Applications, vol. 10, no. 3, pp. 275–287, 2005.
5. Hunter, T., Nosratinia A.: Cooperation diversity through coding. In: IEEE International Symposium on Information Theory, 2002. Proceedings, 2002.
6. Sendonaris, A., Erkip, E., Aazhang, B., Inc, Q., Campbell, C.: User cooperation diversity. Part I. System description. In: IEEE Trans. Commun., vol. 51, no. 11, pp. 1927–1938, 2003.
7. Sendonaris, A., Erkip. E., Aazhang, B.: User cooperation diversity. Part II. Implementation aspects and performance analysis. In: IEEE Trans. Commun., vol. 51, no. 11, pp. 1939–1948, 2003.
8. Cui, S., Goldsmith, A., Bahai, A.: Energy-efficiency of MIMO and cooperative MIMO techniques in sensor networks. In: IEEE J. Sel. Areas Commun., vol. 22, no. 6, pp. 1089–1098, 2004.
9. Jayaweera, S.: Virtual MIMO-based cooperative communication for energy-constrained wireless sensor networks. In: IEEE Trans. Wireless Communications, vol. 5, no. 5, pp. 984–989, 2006.
10. Pabst, R., Walke, B., Schultz, D., Herhold, P., Yanikomeroglu, H., Mukherjee, S., Viswanathan, H., Lott, M., Zirwas, W., Dohler, M., et al.: Relay-based deployment concepts for wireless and mobile broadband radio. In: IEEE Commun. Mag., vol. 42, no. 9, pp. 80–89, 2004.
11. Soldani, D., Dixit, S.: Wireless relays for broadband access [radio communications series]. In: IEEE Commun. Mag., vol. 46, no. 3, pp. 58–66, 2008.
12. Multiprotocol Label Switching (MPLS) Label Stack Entry: "EXP" Field Renamed to "Traffic Class" Field. In: RFC 5462.
13. 3GPP Technical Specification [TS 36.3xx Series]: Evolved Universal Terrestrial Radio Access (E-UTRA) and Evolved Universal Terrestrial Radio Access Network (E-UTRAN); Overall description.
14. 3GPP Release 9 Technical Specification [TS 23.251 version 9.2.0]: Universal Mobile Telecommunications System (UMTS); LTE; Network sharing; Architecture and functional description.
15. Petrov, S.: MPLS Traffic Protection. In: Proceedings of the International Conference on Computer Systems and Technologies CompSysTech’06, Bulgaria, 2006, p. II.18-1-II.18-5.
16. Faisal, A., Saqib, R., Dogar, .F., Ahmad, I., Uzmi, .Z., Ajmone., M., Giuseppe, B., Marco, L., Michela, M, NPP: A Facility Based Computation Framework for RestorationRouting Using Aggregate Link Usage Information, QoS-IP 2005, February 2005.
17. Raza, S., Aslam, F., Uzmi, Z.A.: Online routing of bandwidth guaranteed paths with local restoration using optimized aggregate usage information. In: ICC 2005. 2005 IEEE International Conference on Volume 1, Issue, 16-20 May 2005 Page(s): 201 - 207 Vol. 1.
18. Li, L., Buddhikot, M.M., Chekuri, C., Guo, K: Routing bandwidth guaranteed paths with local restoration in label switched networks. In: IEEE Journal on Volume 23, Issue 2, Feb. 2005 Page(s): 437 – 449.
19. Fast Reroute Extensions to RSVP-TE for LSP Tunnels networks.In RFC-4090, http://tools.ietf.org/html/rfc4090.
20. Virk, A., Boutaba, R., Haque, A..: A Framework for Survivability in Data-Centric Optical Networks. In: Special Edition on IEEE communication magazine.
21. http://www.rfc-editor.org/rfc/rfc2849.txt
22. http://sourceforge.net/projects/mpls-linux/
23. http://www.rfc-editor.org/rfc/rfc2608.txt
24. Kauffman, D., Kauffman, R.: MPLS Technology and Applications. ISBN: 1558606564.
25. Armitage, G.: .QoS in IP Networks. Foundations for a Multi-Service Internet. Macmillan Technical Publishing. ISBN: 1578701899.

26. Huston, G.: Internet Performance Survival Guide. QoS Strategies for Multiservice Networks. ISBN: 0471378089.
27. Rosen, E., Viswanathan, A., Callon, R.: Multiprotocol Label Switching Architecture. In: RFC 3031, Jan. 2001.
28. Mannie, E.: Generalized Multi-Protocol Label Switching (GMPLS) Architecture. In: RFC 3945, Oct. 2004.
29. Lang, J.P., Drake, J.: Mesh Network Resiliency using GMPLS. In: Proc. IEEE, vol. 90, no. 9, pp. 1559-1564, Sept. 2002.
30. McDonald, J.C.: Public Network Integrity-Avoiding a Crisis in Trust. In: IEEE J. Selected Areas in Comm., vol. 12, no. 1, pp. 5-12, Jan. 1994.
31. Iraschko, R.R., Grover, W.D.: A Highly Efficient Path-Restoration Protocol for Management of Optical Network Transport Integrity. In: IEEE J. Selected Areas in Comm., vol. 18, no. 5, pp. 779-794, May 2000.
32. Wang, J., Sahasrabuddhe, L., Mukherjee, B.: Path versus Subpath versus Link Restoration for Fault Management in IP-over-WDM Network: Performance Comparisons Using GMPLS Control Signaling. In: IEEE Comm. Magazine, vol. 40, no. 11, pp. 80-87, Nov. 2002.
33. Markopoulou, A., Iannaccone, G., Bhattacharrya, S., Chuah, C-N., Diot, C.: Characterization of Failures in an IP Backbone. In: Proc. IEEE INFOCOM ’04, vol. 4, no. 7-11, pp. 2307-2317, Mar. 2004.