A Quantitative Comparison of Some Resilience Mechanisms in a Multidomain IP-over-Optical Network Environment

D. Staessens, L. Depré, D. Colle, I. Lievens, M. Pickavet, P. Demeester.
Ghent University – IBBT – IMEC, Department of Information Technology
Gaston Crommenlaan 8, 9050 Gent, Belgium
E-mail: {dimitri.staessens, leen.depre, didier.colle, ilse.lievens, mario.pickavet, piet.demeester} @intec.ugent.be

Abstract— **When we examine today's internet architecture, we notice that the IP layer network is divided into multiple domains, managed by different service providers, operating different architectures, providing different services, handling different business strategies. In order to provide survivable inter-domain connections, to ensure connectivity in case of the most prevalent failures, different strategies can be followed. In this paper, we present some multidomain resilience schemes for a single optical backbone network interconnecting different IP domains. We then present a quantitative study of the network capacity required, in a specific pan-European backbone network.**

Index Terms— **Multilayer networks, Multidomain survivability, Protection, Recovery**

I. Introduction

Today, optical backbone networks provide the physical transmission medium for internet, voice and multimedia traffic. With the advent of WDM technology, the amount of data traversing these networks is tremendous [1]. Fast and scalable network recovery techniques are of paramount importance in order to provide the increasingly stringent levels of reliability network operators are demanding for their future networks [2]. This is even more so for backbone network operators, interconnecting different IP domains, because critical failures could lead to the isolation of entire IP domains. Up to now, most resilience mechanisms are developed for single-domain environments, which can be used more or less effectively in the current hierarchical network structure. However, in the near future peer-to-peer type network connections are expected to increase significantly, causing a flattened network structure with many networks on the same level. This means that end-to-end traffic will traverse through different layers of different networks and the end-to-end resilience can only be provided if interworking between different networks and network layers is considered in the resilience mechanism.

Manuscript submitted February 15, 2006.
This research was partly funded by the European Commission through the IST-projects NOBEL and e-Photon/ONe and by the Flemish Government through the projects IWT-GBOU ONNA and FWO G.0315.04.

There has been some research effort towards the interconnection [3] and protection [4] of different optical domains. Interconnection of domains on the network layer level, using different network layer protocols and MPLS has been studied in e.g. [5],[6]. In [4], three dedicated schemes for optical protection are evaluated with regard to blocking probability of lightpath requests through interconnected optical networks. These schemes are: Basic end-to-end, Disjoint Segment and Concatenated Segment. We remark that the first scheme requires total knowledge of the network topology; the second scheme requires certification that two *domain-disjoint* networks are also *physically* disjoint. (It is somewhat naïve to simply assume this to be true, e.g. different operators may use the same bridge for their physical links to cross a river), and the third scheme is only link-disjoint, and does not cover gateway failures.

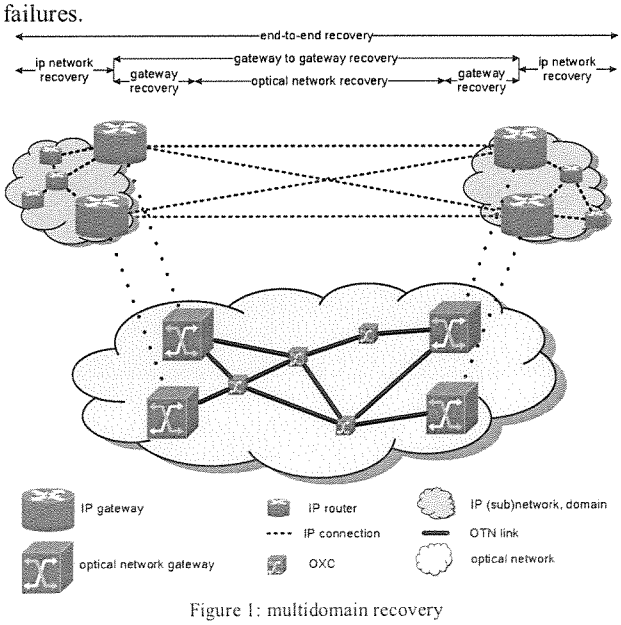

Figure 1: multidomain recovery

Figure 1 shows the hierarchy of recovery options within multidomain IP networks, interconnected by an optical domain. To provide end-to-end protection within a multi-layer environment, we can try to use existing recovery techniques within the different sections (IP network recovery, gateway

1-4244-0355-3/06/$20.00 (c) 2006 IEEE
This full text paper was peer reviewed at the direction of IEEE Communications Society subject matter experts for publication in the IEEE ICC 2006 proceedings.

recovery and optical network recovery) and provide proper coordination between them in order to achieve end-to-end protection and ensure inter-domain connectivity in case of single network node or link failures.

In the following sections, several generic approaches for providing end-to-end recovery in a multidomain IP environment over an optical backbone network will be presented. We concentrate on the recovery within the optical domain, and implicitly assume that recovery within the IP domains is provided. A quantitative comparison between the different methods will be given in section III.

II. Generic Multidomain Recovery Approaches

This section discusses the provisioning of recovery functionality in multilayer multidomain networks by starting from an IP-layer-only recovery scheme and then introducing optical protection. Note that, in order to ensure connectivity, each domain needs at least two gateways to serve as entry-points into the backbone network. In case of a failure of one of these entry-points, another is available to take over. After the IP-only recovery, improvements towards recovery times and capacity requirements are suggested. Finally, we introduce two dynamic recovery methods, based on global recovery.

A. No optical protection

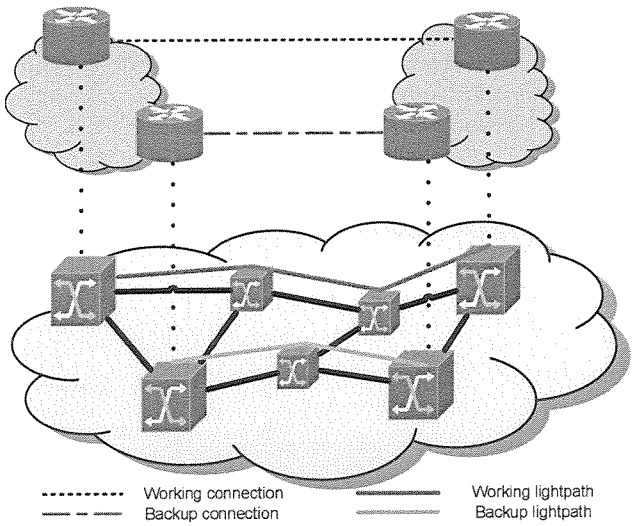

Figure 2: no optical protection

We interconnect the different domains using two IP connections between two distinct gateways in each domain-pair, which will be referred to as the working and backup connection. In this scenario, the IP connections are implemented as unprotected node-disjoint lightpaths in the optical domain (Figure 2). This scheme provides full protection against single node or link failures in the optical backbone network, but requires an MPLS capability in each IP domain in order to switch over from the working connection to the backup connection in case of a failure in the working lightpath. In absence of MPLS, the IP layer will have to converge to the new topology without the working connection, which will have some down-time as a result. From the point of view of the backbone operator, any single node failure will affect ±50% of the working connections between different domains (clients). So in absence of MPLS in the IP domains, this scenario will not be the best option.

In case of the setup of two IP connections between a domain-pair, the choice of which gateway to connect to another gateway is not arbitrary when a node disjoint path is required for protection. This is illustrated in Figure 3 below: there is no node-disjoint implementation of IP connections *a-c* and *b-d*, however, if we connect *a* to *d* and *b* to *c*, node disjoint lightpaths can be implemented in the optical domain.

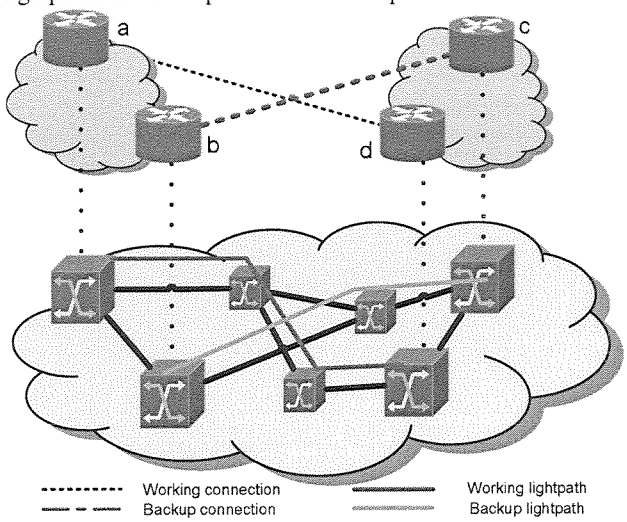

Figure 3: node disjoint implementation of IP links

This restriction has a serious impact on how multidomain protection should be realized. Since network operators aren't keen on disclosing details about their networks, there are two options: a special multidomain multi-layer discovery protocol should determine on-the-fly which gateways to connect (without disclosing internal topology information), or the IP operator asks for node-disjoint connections, and the backbone operator then replies with how the routing tables in the IP gateways should be set up (in our example above, *a-d* and *b-c*).

B. Protecting both lightpaths optically

In order to provide a more robust domain interconnection, and resolve the issue of down-time during IP-connection switchovers, the backbone operator can choose to protect every lightpath optically. The optical protection lightpaths for the working and backup lightpath will be called primary and secondary backup lightpath respectively. It should be kept in mind that in all of the following scenarios, the working and backup lightpath aren't necessarily link - or node-disjoint.

The working and backup lightpath can be implemented as two shortest paths between two distinct gateways, and protected with optical 1+1 path protection. In this case, the connections between two domains are protected twice, in the IP domain from the multidomain point of view, and in the optical layer of the interconnection domain. This scheme has the upside that, in case of a non-gateway failure, the IP links aren't

disturbed, so only a critical gateway failure (or a failure of the interface between the gateway OXC and IP gateway) will lead to potential downtime in the absence of an MPLS control plane. As a downside we may expect a lot of capacity overhead required in the backbone network (Figure 4).

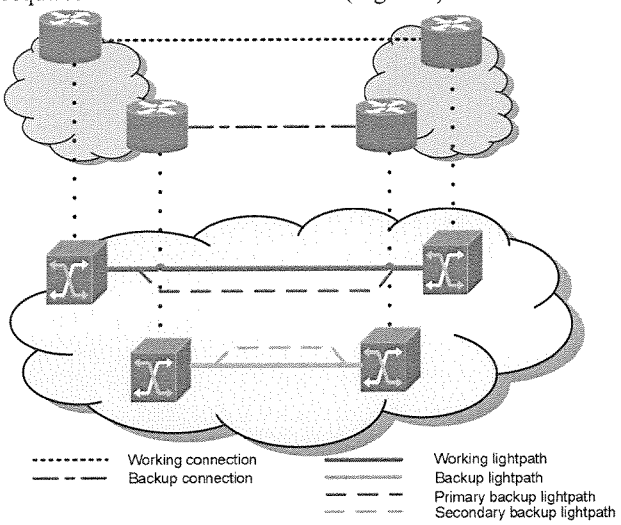

Figure 4: double protection

In order to reduce the required network capacity, the operator can apply capacity sharing [7] between both backup lightpaths (Figure 5) and between backup lightpaths of different domain-pairs (not shown). A downside is that it's not possible to do 1+1 protection of the data by simultaneously sending it over both the primary and secondary path.

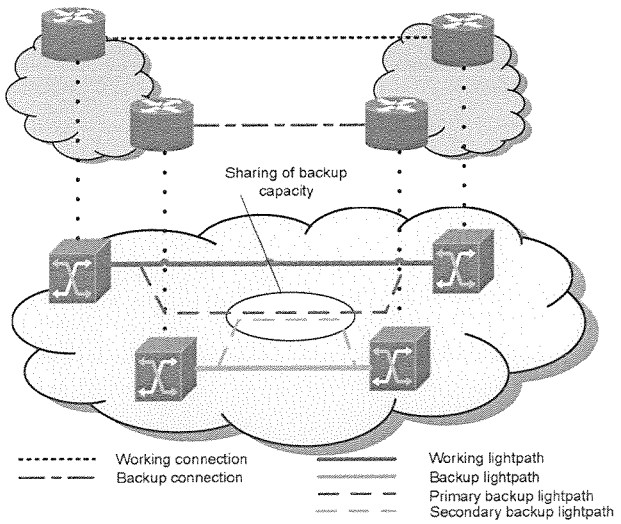

Figure 5: double shared protection

C. *Protecting only the working connection*

In the previous options, the choice between working connection and backup connection is somewhat arbitrary. In fact, it is possible to divide the traffic over both connections, and have the same level of protection. If we make a more formal choice between working and backup connection, then there is no need to protect the backup lightpath optically, since a failure along its path will not disturb any working connections. If only the working path is protected optically the operators should make concrete decisions on which gateways are primary and which routers are used as backup for every inter-domain connection. The reason why routers should be declared for every inter-domain connection is that a gateway must be able to serve as primary gateway for some connection while serving as backup for another.

It is possible to further reduce capacity requirements by allowing the primary backup lightpath to preempt the backup lightpath (Figure 6). This is referred to as *common pool* capacity sharing [8]. This is because the backup lightpath will only be used when an unrecoverable failure in the working lightpath occurs, i.e. a gateway failure. In case of a failure in the working lightpath, the backup IP link is torn down, but the working IP connection remains intact.

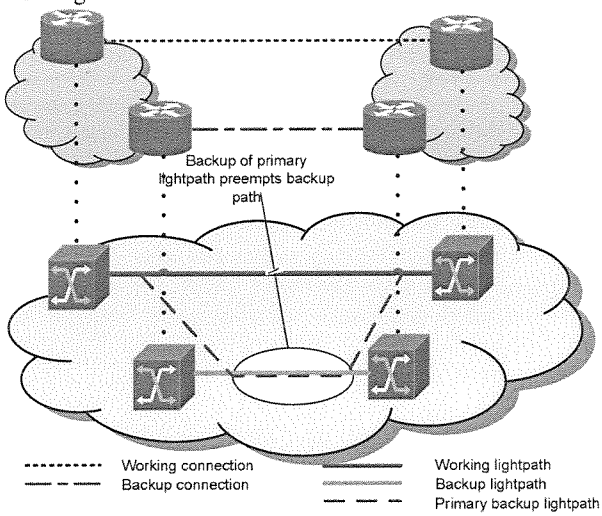

Figure 6: working lightpath protection with backup path preemption

D. *Dynamic restoration*

In this subsection, we consider dynamic restoration on an Automatically Switched Transport Network (ASTN[9]), more specifically, an Intelligent Optical Network (ION). In this case, the optical layer tries to reroute all traffic among the available links and routers after a failure. These lightpaths aren't protected optically. In a first scenario, we set up two paths between each domain-pair, and let the ION resolve failures in *both* IP connections, in other words, it will try to restore both the primary and the backup lightpaths (Figure 7).

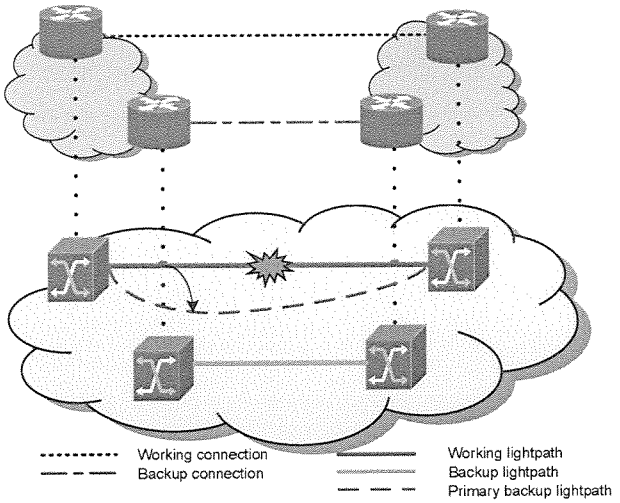

Figure 7: 2-path dynamic restoration

We can also choose to set up only one path, and, in case of a gateway failure, route the traffic over another gateway. This scenario is highly specific for multidomain survivability, since the traffic originating (from the interconnection provider point of view) in the failing gateway can in fact be recovered, which is not possible in conventional single-domain networks (Figure 8).

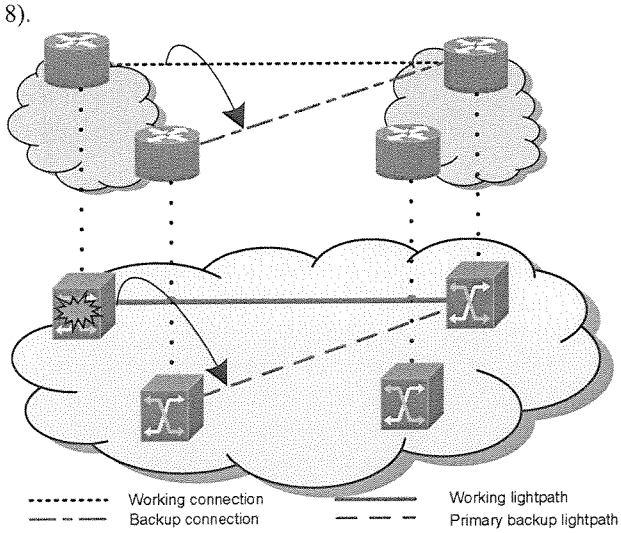

Figure 8: working lightpath dynamic restoration

It should be noted that in order to provide this type of recovery in real-world situations, a reliable protocol needs to be developed with extensive signaling between IP domain and backbone network.

III. Case Study

A. Simulation setup

We evaluated these resilience options on the e1 multidomain network [10], with a backbone network connecting the different domains.

In order to study the above scenarios, we needed to define a backbone network to perform our cost analysis. The requirements were that all IP domains in the e1 network should be interconnected; every IP domain had at least two interfaces towards the optical backbone in order to ensure connectivity in case of an IP or Optical gateway failure (Figure 9). It has 41 nodes and 61 links (average degree 2.97). The minimum degree is 2, the maximum degree is 5. One adaptation we made on the e1 multidomain network was to aggregate Croatia and Slovenia into a single domain, (with Zagreb and Ljubljana as gateways), in order to get at least two gateways per domain in the core network. All other domains are national networks; all nodes depicted within the country are gateways for that national network, except for Bilbao and Bordeaux (these were added to provide the connectivity required). There are no single points of failure within this backbone network.

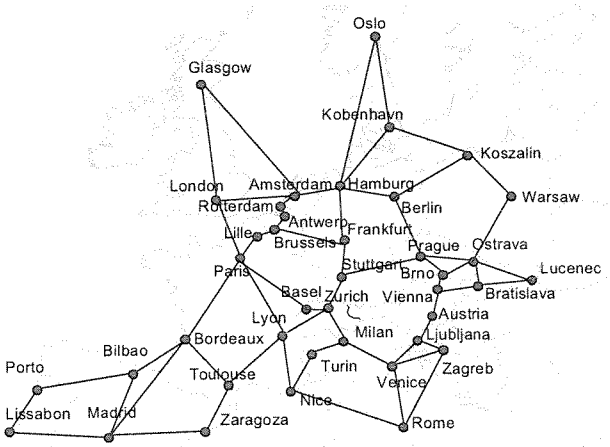

Figure 9: interconnection domain

Traffic for the simulations is taken from the elnet traffic matrix [10], and routed as STM-16 traffic over the network. The traffic is considered to be symmetrical between domains, which is reasonable since peer-to-peer traffic is becoming the most prevalent type of traffic in computer networks.

B. Performance analysis method

For each of the aforementioned scenarios, we computed the total link capacity requirements for the backbone network. We determined the pairs of gateways, to be connected for each domain-pair, with a shortest cycle algorithm. This is in order to ensure of the possibility of node disjoint lightpaths in the optical domain, as discussed in section II.A. We used these gateway-pairs to setup the gateway-to-gateway IP connections in all of the discussed scenarios, even in scenarios where node-disjoint lightpaths weren't required. This does not mean that each domain has exactly two gateways, it only means that we connect domain A with B using the same gateways throughout all scenarios. For the connection of domain A with C, A may use different gateways (but always the same throughout the different scenarios). Optically protected paths were also computed with the shortest cycle algorithm,

unprotected paths are simply shortest paths.

For the dynamic recovery options, we considered a global restoration mechanism, i.e. we recovered the failure by computing an entirely new path for every connection over the network. There is also an option to do local recovery, which requires computation of a new route only for aversely affected traffic in the direct neighborhood of the failure.

Note that in the static case, the calculated capacity is always a direct indicator for the total network cost. In the dynamic case, this is not always true, since it is possible to share IP capacity over different failure scenario's [11]. As shown in [12], local dynamic recovery will usually reduce the network cost compared to global dynamic recovery, due to savings in the IP layer because of the reduction in required reconfigurations. In our study presented here, we consider the interconnection domain to be entirely constituting of optical equipment, i.e. the IP equipment is in the hands of other operators. IP capacity requirements for the gateways will therefore be evaluated independently. We will show that for almost all cases the IP capacity requirement is the same.

C. *Simulation results*

When we compare the total capacity requirements against each other, we see that optical protection will always require extra capacity in the backbone network (Figure 10). We have normalized the results versus the optically unprotected scheme. The higher we share backup capacity between backup paths and the more intelligently we provide protection (e.g. by not protecting backup connections optically), the less capacity we need in order to ensure connectivity between different domains.

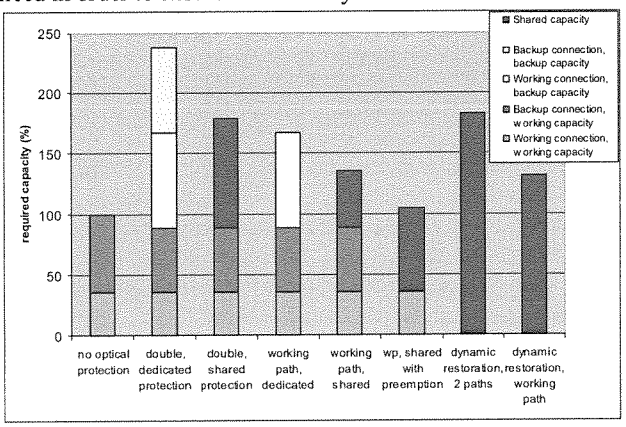

Figure 10: relative capacity requirements

In Figure 10 we have differentiated, where possible, the required optical capacity in 5 categories, namely Working Connection Working Capacity (WCWC), Backup Connection Working Capacity (BCWC), Working Connection Backup Capacity (WCBC), Backup Connection Backup Capacity (BCBC) and Shared Capacity (SHDC)

Taking a closer look at Figure 10, we can clearly see the gain of sharing capacity. In the unprotected scheme, we only have two dedicated lightpaths. When we apply dedicated optical protection to these, we gain a little capacity, because both paths needn't be disjoint. However, protecting both paths is very costly. When we apply sharing between the backup lightpaths, we again gain a lot of capacity. The SHDC part of the third option can route the same paths as WCBC and BCBC from the second option, however, not both at the same time. This is our most efficient symmetrical scheme. Note that in schemes 2-5, the WCWP and BCWC bars are exactly the same. When we abandon symmetry and explicitly specify which connection is to be used as working connection, we can restrain from protecting the backup path, again resulting in a capacity gain. Note that both bars in the second and fourth option are exactly the same, except, of course, for the BCBC part. Now, sharing between the WCBCs of different domain-pairs reduces the total capacity requirement again, and letting the WCBC use the BCWC, by preempting the backup path, leaves us with the most efficient scheme regarding capacity-requirement, requiring only about 7% extra capacity when compared to providing no optical protection.

For the dynamic protection schemes, differentiation is nigh impossible.

When we look at the IP line card requirements (Figure 11), we can see that dynamic recovery of the working path has no capacity advantage over static recovery. When we assume that the total traffic between the domains is 3 lightpaths, we set up two connections *a-c* and *b-d*, each requiring 3 lightpaths in the static case. For the dynamic case, we must consider all failure scenarios [13]. In the failure-free scenario, we need 3 IP capacity in routers *a* and *c*, since we only set up connection *a-c*. When router *a* fails, we tear down lightpaths *a-c* and set up 3 lightpaths for the new connection *b-c*, so router *b* needs capacity 3, but we can reuse the 3 free IP cards in router *c*. Similarly, a failure of router *c* leads to the setup of *a-d* and *d* needs capacity 3.

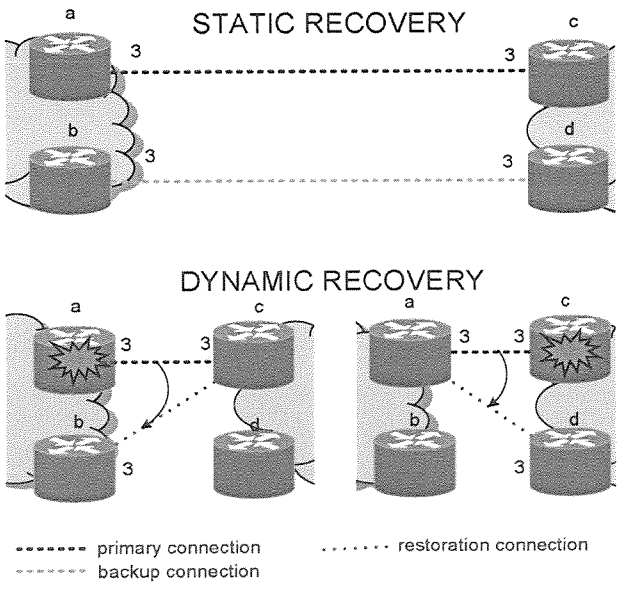

Figure 11: IP capacity requirements

A failure in gateway *b* or *d* does not require rerouting, so, in both the static as working-path-dynamic case, all IP routers need capacity 3. This is a very useful fact regarding protocol design, and implementation, because the gateways require the

same capacity for each scheme.

Setting up both working and backup connection dynamically requires more capacity in the dynamic protection scheme than with static provisioning. As just explained, we need capacity 3 in the IP layer for the static scheme. The calculation for the dynamic scheme is shown in Figure 12, which shows that the IP capacity requirement is in fact 6 per IP gateway. This is a result only applicable for multidomain IP networks, and a direct consequence of the fact that IP traffic 'originating' (from the optical backbone point of view) in a gateway can be recovered in another gateway.

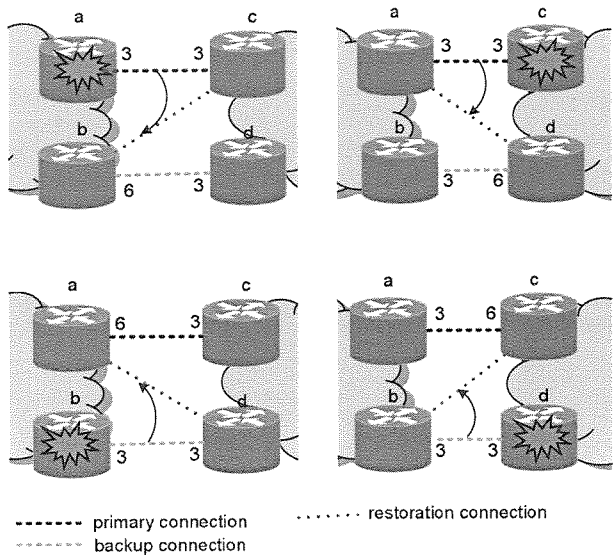

Figure 12: dynamic restoration of two paths

Dynamic restoration can provide a solution to the simultaneous failures of routers *a* and *d*, for example, where our static recovery cannot. The drawback is that dynamic restoration can require IP re-convergence, which takes quite some time [14]. Dynamic restoration of both paths is inefficient regarding networking resources. Furthermore, the resulting backup connection is not gateway-disjoint, and therefore practically useless.

IV. Conclusions

In this paper, we have presented several ways to protect the interconnection of different IP domains over an optical backbone. We started from a simple setup where the IP domains are connected statically with two optically unprotected IP connections. We then introduced optical protection of these IP connections and used different levels of sharing to reduce capacity requirements for the optical interconnection domain. After that, we have investigated two dynamic protection mechanisms, one where we setup working and backup connections per domain-pair, and another where we setup only the working path.

A quantitative comparison of these resilience strategies shows that sharing of capacity in the optical layer has a significant impact on the total capacity requirement for the backbone network. We also showed an unexpected result in the considered multidomain strategies, namely that dynamic recovery does not improve the IP layer capacity requirements; in fact, setup of working and backup path requires more IP capacity in the dynamic case than in the static case. This is a direct consequence of the multidomain nature of the network, where we can setup a working and backup connection originating and terminating in different gateways.

V. Directions for Further Study

Further study could reveal some interesting consequences of using more than two gateways per domain, sharing the IP capacity of the gateways and dividing the traffic over them. Other extensions are towards a more diverse topology and extending the paths across multiple domains, using one of the proposed schemes in each domain. Ideally, there should be a single protocol, called at each border between gateways, able to set up such survivable connections.

References

[1] Nico Wauters, Gzim Ocakoglu, Kris Struyve and Pedro Falcao Fonseca, "Survivability in a New Pan-European Carriers' Carrier Network Based on WDM and SDH Technology: Current Implementation and Future Requirements," IEEE Comm. Mag., vol. 6, no. 8, pp. 63-69, Aug 1999.

[2] Jean-Philippe Vasseur, Mario Pickavet and Piet Demeester, "Network Recovery," San Francisco: Morgan Kaufmann, 2004.

[3] Admela Jukan et al., "End-to-End Service Provisioning in Multi-granularity Multi-domain Optical Networks," 2004 IEEE International Conference on Communication (Optical Networking Symposium), Paris, June 2004.

[4] Srinivasan Seetharaman et al., "End-to-End Dedicated Protection in Multi-Segment Optical Networks," http://www.cc.gatech.edu/grads/s/Srinivasan.Seetharaman/papers/e2eprot.pdf

[5] Thomas Engel, et al., "Increasing End-to-End Availability over Multiple Autonomous Systems," PDPTA'05 June 2005 Las Vegas, USA.

[6] Thomas Schwabe et al., "Resilient Routing Using ECMP and MPLS," *HPSR 2004*, April 2004 Phoenix, AZ, USA.

[7] Piet Demeester et al., "Resilience in multi-layer networks," IEEE Communications Magazine, vol. 37, no. 8, August 1998, pp. 70-76.

[8] M.Pickavet et al., "Recovery in Multilayer Optical Networks", IEEE J. Lightwave Technology, vol. 24, No.1, January 2006.

[9] ITU-T Recommendation G.807/Y.1302, "Requirements for automatic switched transport networks (ASTN)," ITU-T Standardization Organization, July 2001, www.itu.int.

[10] http://qosip.tmit.bme.hu/~mesko/e1net.

[11] Sophie De Maesschalck et al., "Pan-European optical transport networks: an availability based comparison," Photonic Network Communication, vol. 5, no. 3, May 2003, pp. 203-225.

[12] Sophie De Maesschalck et al., "Intelligent Optical Networking for Multilayer Survivability," IEEE Communications Magazine, vol. 40, no. 1, January 2002, pp. 42-49.

[13] Adelbert Groebbens et al., "Logical Topology Design For IP Rerouting: ASONs versus static OTNs," submitted to Photonic Network Communications (2005).

[14] Christian Guillemot, "VTHD French NGI Initiative: IP and WDM Interworking with WDM Channel Protection," presented at the 2000 IP over DWDM conf.


www.icc2006.org
IEEE International Conference on Communications
11-15 June 2006
IEEE Catalog Number: 06CH37799C
ISBN : 1-4244-0355-3
Library of Congress : 81-649547
IEEE
IEEE COMMUNICATIONS SOCIETY
ICC 2006
İSTANBUL
Bridging Continents Through Communications
Copyright © 2006 IEEE