Assessment of Resilience Features for the DPT Rings[1]

Salvatore Spadaro, Josep Solé-Pareta, Davide Careglio

Universitat Politècnica de Catalunya (UPC), Advanced Broadband Communications Center (CCABA), Barcelona, Catalunya (Spain)

spadaro@tsc.upc.es, {pareta, careglio}@ac.upc.es

&

Krzysztof Wajda, Andrzej Szymanski

University of Mining and Metallurgy (AGH), Krakow, Poland

szymans@uci.agh.edu.pl, wajda@kt.agh.edu.pl

Abstract

An outage of the network infrastructure can imply serious consequences, both economical and social, for the Network Operators. Thus, the provision of resilience mechanisms able to maintain service availability even under failure conditions is crucial. In order to be robust, the network has to be reconfigurable. The reconfiguration should be both fast and cost-efficient. This paper tests the recovery mechanism provided by Dynamic Packet Transport technology introduced by Cisco Systems, which is the starting point of the standardization effort currently carried out by the IEEE Resilient Packet Ring Study Group (RPRSG) towards the establishment of a new IEEE standard, the IEEE 802.17. Both theoretical and simulation studies are addressed in this paper. In the theoretical part, the special cases of worst traffic streams assignment, which lead to significant degradation of the DPT ring efficiency after a failure, are discussed. For the simulation studies, two case studies were carried out, one aiming to test the recovery time of DPT resilience features in realistic traffic conditions, and. the other to verify theoretically described worst cases.

1. Introduction

DPT (Dynamic Packet Transport) is an emerging transport technology, which attracts engineers by its simplicity, distributed management, support for QoS, and enhanced resilience features. DPT offers flexible bandwidth sharing by using SRP-fa protocol and it is a ring-based optical network, which enhances efficiency and provides powerful resilience mechanisms for certain failures that occur in the network.

DPT is based on two symmetric counter-rotating optical rings (Figure. 1-a) and it is meant to be used as a metropolitan and wide area network solution providing innovative and optimised network architecture for ring-based delivery of IP services. DPT is based on two protocols [2], namely SRP (Spatial Reuse Protocol), responsible for selective bandwidth reuse in the ring, enhanced by a new mechanism supporting fairness in bandwidth sharing among nodes (the SRP-fairness algorithm), and IPS (Intelligent Protection Switching), responsible for providing resilience by ring wrapping after a failure has occurred (Figure. 1-b). DPT fundamentals (SRP-fa and IPS) are completed by the topology discovery (TD) procedure and an optimal path selection, performed after ring reconfiguration.

---

[1] This work has been partially funded by the European Commission under the Information Society Technology (IST) program, (LION project, IST-1999-11387), and by the CICYT (Spanish Ministry of Education) under contract TIC99-0572-C02-02

In comparison with the currently enabled technology, which DPT pursues to substitute (i.e., SONET/SDH rings), DPT exhibits the following advantages [1]: 1) Increases bandwidth efficiency by implementing the spatial reuse of bandwidth and the statistical multiplexing of packets, 2) Reduces costs and complexity by eliminating intermediate layers between the IP layer and the optical layer. Also, it has to be noted that DPT equipment should be less expensive than SONET/SDH equipment, 3) DPT enables service integration by supporting traffic priorities, so such services as voice and video over IP can be transparently sent over campus, metropolitan and wide area networks, 4) overcomes the limitations that TDM/circuit-based architectures impose on data communications allowing direct connectivity without circuit provisioning. Furthermore, DPT was designed to provide analogous self-healing properties than the Automatic Protection Switching (APS) of SONET/SDH networks, and the wrapping of traffic onto the alternate path is done without the need to allocate back-up resources.

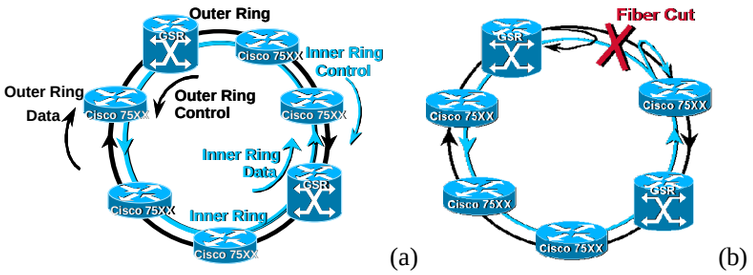


Figure 1 a) Dynamic Packet Transport, b) IPS recovery mechanism

IEEE recognized unique features of DPT. Currently there is a standardization effort in the IEEE Resilient Packet Ring Study Group (RPRSG) with the aim to establish of a new IEEE standard, the IEEE 802.17 (this work started officially in March 2000 and mature standard will be probably available in autumn this year). RPR is considered as a technology that constitutes a superset of features previously predefined for DPT. These efforts prove that DPT (and its successor - RPR) has interesting features concerning transport efficiency and resilience.

In previous works the performance of the SRP-fa protocol was evaluated [3], and the problem of behaviour of DPT rings under high load conditions and different LO/HI traffic streams was studied [6,7]. This paper deals with the resilience features of DPT in an IP/DPT/OTN scenario (OTN stands for Optical Transport Network) studied under the scope of LION European Fifth Framework Programme project. Furthermore, were studied recently.

The reminder of this paper is organized as follows. Section 2 contents a short review of the DPT resilience features. Section 3 presents a theoretical study of the worst traffic streams assignment cases, those that may lead to the significant degradation of the DPT ring efficiency after a failure. Sections 4 and 5 include two different case studies carried out by simulation, both aiming to evaluate the time required for a DPT network to return to the steady state after a link or node failure under different traffic conditions. Finally, Section 6 concludes the paper.

2. DPT Resilience Feature

As mentioned, DPT is based on two protocols [2]: SRP (Spatial Reuse Protocol), responsible for selective bandwidth reuse in the ring, enhanced by a new mechanism supporting fairness in bandwidth sharing among nodes, SRP–fa (SRP – fairness algorithm), and IPS (Intelligent Protection Switching), responsible for providing resilience by ring wrapping after the failure has occurred. This Section is devoted to shortly review the features of the latter protocol.

2.1. Intelligent Protection Switching Protocol

IPS is a protocol to automatically recover from ring failures, and line (span) degradation problems. It provides proactive performance monitoring. IPS is analogous to the self-healing properties of SONET/SDH (APS) but the wrapping of traffic onto the alternate path is done without the need to allocate protection bandwidth (back up resources). If a failure is detected (either a link or a node failure),

packets directed towards the failure are wrapped back in opposite direction (Figure 1-b). Wrapping is made possible because of the internal node hardware with dual homing (connection to inner and outer ring). IPS controls wrapping in the nodes adjacent to failed span or equipment (node). IPS acts by wrapping rings in the node, which recognized the failure (or signal degradation). There are a few methods of gaining information about failure or signal degradation, both internal and external [2]. The internal (independent from lower layers) sources of information for IPS are: 1) A number of CRC checksum errors above a specified threshold (which indicates either signal degradation or complete link failure). 2) The SRP control packets (usage packets), which act as a keep-alive mechanism (sent periodically at interval of approx. 106 µsec, the loss of 16 consecutive usage packets triggers protection mechanism).

The information about a failure can be provided to DPT layer by lower layers; for example, SDH or OTN alarms. DPT network element supports SONET/SDH MIB [5] to signal alarms, events and performance monitoring information according to [4].

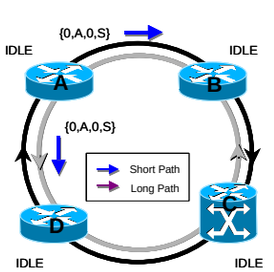
The IPS protocol maintains a protection switching event hierarchy that handles concurrent multiple events (e. g. signal fail and signal degrade events) without partitioning the ring into separate sub-rings. Figure 2-a lists the request types ordered from the highest to lowest priority.

In order to maintain this protection request hierarchy, each node, with respect to the IPS protocol, can be in one of the following states: 1) *IDLE*: the node is ready to perform a protection switch. 2) *PASS-THROUGH*: the node enters this state when it receives a long path IPS packet. 3) *WRAPPED*: the node enters this state when it receives a local request or detects a fault or receives a short path IPS packet from an adjacent node. In this state, the node performs the ring wrap.

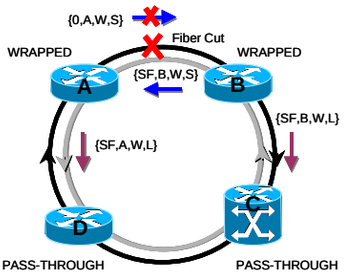
Figure 2-b shows an example of how IPS works. The example shows a DPT ring composed of four nodes in which a fibre cut on the fibre from node A to B is considered. IPS control messages are figured as {Request type, Source Address, Wrap Status, Path Indicator}.

Priority	*Type of request*
1	Lockout of Protection (LO)
2	Forced Switch (FS)
3	Signal Fail (SF)
4	Signal degrade (SD)
5	Manual Switch (MS)
6	Wait to Restore (WTR)
7	No Request (IDLE)

(a)



(a) Ring in Idle



(b) Single Fiber Cut Scenario

(b)

Figure 2 a) Protection request hierarchy, b) IPS operation

In absence of failure ("ring in idle"), each node periodically sends an IPS message (IDLE). When a fibre cut occurs in the outer ring between A and B, node B detects a signal fail (SF) on the outer ring, (e. g. not receiving the periodic Usage message from node A). Thus, it changes to Wrapped state performing a wrap and transmits towards A on the inner ring (short path) the message {SF, B, W, S} and on the outer ring (long path) the message {SF, B, W, L}. Node A after receiving a protection request from node B on the short path changes to Wrapped state. Then, it transmits towards B on the short path {0, A, W, S} and on the long path {SF, B, W, L}. When the nodes C and D receive long path IPS packets (switch requests), they change from Idle to Pass-through mode (in each direction). It has to be noted that IPS long path messages are not used to wrap up the ring.

2.2. Topology Discovery Protocol

The Topology Discover protocol (TD) [2] is used for the network reconfiguration after the wrapping. In normal DPT ring operation, both rings (inner and outer) are utilized to carry traffic. After the ring wraps, the available bandwidth is halved, and low priority data traffic is reconverged fairly to the lowered bandwidth, which is accomplished dynamically by SRP-fa. In order to optimise the bandwidth utilization it is necessary to run the TD protocol because DPT supports basic version of traffic forwarding based on number of spans (shortest path is chosen towards destination DPT node).

Each DPT node performs this action by sending out special discovery packets on one or both rings. The originator of a topology discovery packet sets egress ring identifier (inner or outer ring), adds its own MAC address and length field. Such packet is sent hop-by-hop around the ring (however in nature it is a point–to–point packet). Each traversed node appends its MAC address, updates length field and forwards packet towards destination. After reaching again originator of this packet, topology discovery packet has all nodes MAC addresses in proper order and with relevant length field. This is the basic behaviour of topology discovery mechanism. When sending topology discovery packet over wrapped ring, the wrapped node indicates this situation and wraps the packet (i.e. sends it further along reconfigured ring). On the way towards originator after passing wrapped node, MAC addresses are not added (since this is travelling same route in opposite order of nodes). The topology map of the ring is changed after receiving two identical TD packets. This is done to avoid changes of topology in transient conditions. The delay introduced by the TD protocol is the time of passing whole ring (also being wrapped) plus necessary service of packet inside subsequent nodes.

2.3. Resilience features in an DPT over OTN environment

In a DPT over OTN scenario there are resilience capabilities in both DPT and OTN layers, which provide coverage of broader spectrum of failures compared to single layer resilience. In case of OTN protection only, the failures of DPT equipment are not handled while in case of DPT protection only, each failure results in reducing available bandwidth. When combining DPT and OTN resilience features, we are using technologies with similar reaction times but different features. DPT recovers from failure by wrapping a ring(s) around the failed span while OTN has dedicated resources.

3. Theoretical Studies

The DPT protocol was defined as a fully distributed one, without management facility. However, complex interference between high and low priority traffic services in nodes may lead to some problems. The aim of this section is to show special cases of traffic assignment that can lead to a significant degradation of network performance when a failure occurs and the IPS procedure wraps rings. The following 3 cases are proposed (for further details refer to [9]):

Case 1: Considers low priority (LO) traffic only and analyses the behaviour of DPT before and after failure (Figure 1). The motivation is that in this case traffic is spread evenly and due to basic feature of SRP we get maximum throughput - thus this is highly desired situation. After failure, disregarding the root of failure due to symmetry in the ring, we get the available bandwidth decreased by 50%.

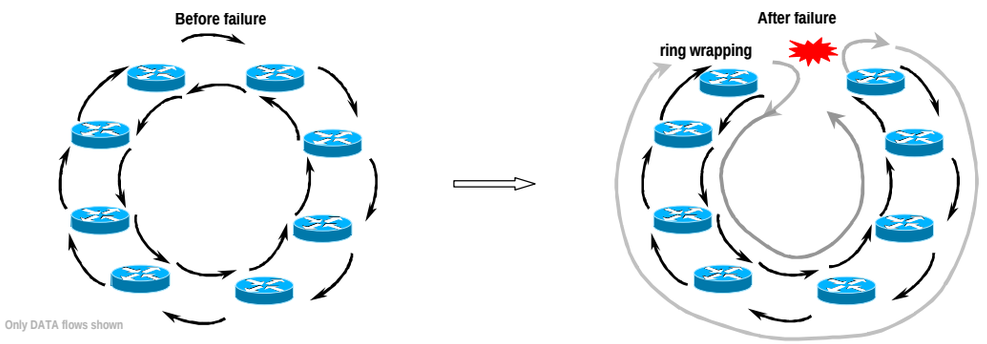


Figure 3 DPT Ring with traffic streams sent to neighbour nodes (fibre rings are not shown)

Case 2: It comes from detailed investigations that a very complex and inconvenient situation is shown in Figure 2. It consists in sending traffic to adjacent nodes in one part (here: right) of ring and to a given node (depicted here as *A* node) in another part of ring. This case seems to be important since detailed analysis shows that for large DPT rings the reduction of capacity after failure can be significant (up to 94%) [9].

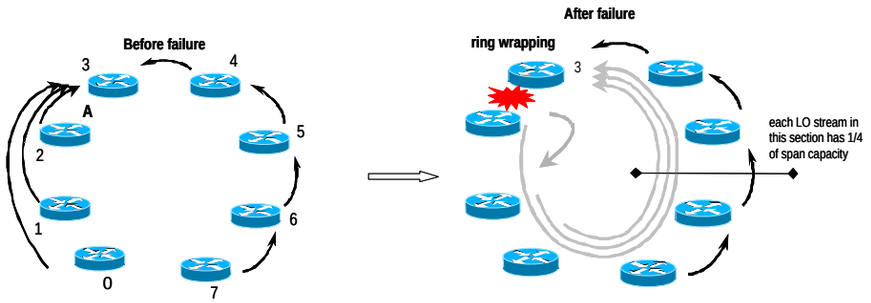


Figure 4 DPT Ring with worst-case traffic streams assignment

Case 3: Discusses a situation where one node is receiving large LO traffic stream. This can be valid for a node working as backup server. For this traffic arrangement, after failure located in the span transmitting the largest number of streams the network capacity is reduced by 50 % [9].

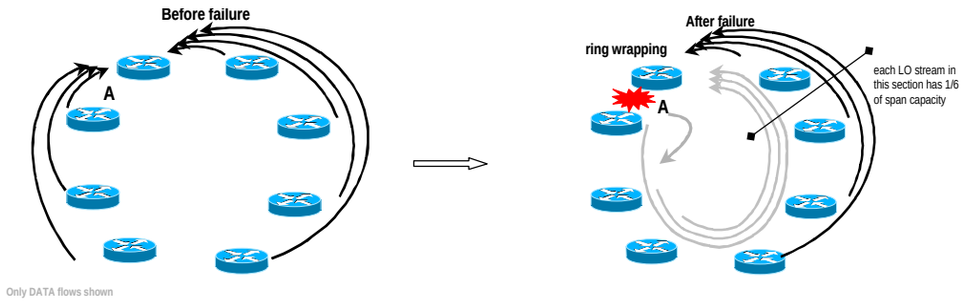


Figure 5 DPT Ring with receiving extensive LO flows from other nodes

4. Simulation Studies: Case study 1

This case study was carried out using a simulator developed in Opnet, which includes the SRP-fa functionalities, the protocol and the TD mechanism. The purpose of this study was to evaluate the recovery time of the DPT resilience features. In particular, it was evaluated the time required for a DPT network to return to the steady state after a link or node failure. This time includes the IPS recovery time (how long the IPS needs to restore the traffic after a failure), the TD reconfiguration time, and the SRP-fa protocol stabilization time.

On one hand, the IPS recovery time includes the detection of the fault, the IPS messages generation and state transitions, and the final ring wrap. As specified in [2], we considered that a failure is detected after loosing 16 consecutive control packets sent at interval of 106 μs. Thus, the time to detect a failure is about 1.7 ms. Therefore, the IPS recovery time is given by 1.7 ms plus the time needed to aware all nodes about the failure by sending them the IPS control messages. On the other hand, the SRP-fa protocol stabilization time is the time required for the SRP-fa protocol to react to the network reconfiguration produced by the TD protocol and return to the steady state.

4.1. Simulation Scenario

The simulated network scenario consisted of a metropolitan IP network. In particular, the scenario is extracted from Milan reality but it can be supposed that it corresponds to many other big European cities. We considered services classes belonging to both elastic (web browsing, http based services and e-mail services) and streaming, with stringent delay requirements (phone services and video streaming). The services considered are the most common IP-based applications.

The simulated network was a DPT ring (two symmetric counter-rotating optical rings) connecting several IP Routers (12), and several Internet Servers (3). This leads to a network with an odd topology, which is depicted in Figure 6.

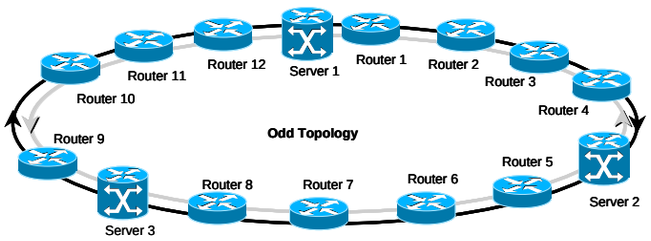


Figure 6 IP network logical topology

The distance between the different nodes was set to 3 km, which means a propagation time between nodes of 15 μsec. We considered an OC-48 (2.5 Gbps) DPT node interface, and video and voice traffic as HP traffic and data traffic (web browsing, http and e-mail services) as LO traffic.

We assumed that the network consists of a logical topology composed by three different segments, each one including four routers logically attached to one server, able to provide the above-mentioned services. It has to be noted that each segment represents a geographical zone of the metropolitan environment. Moreover, we assumed traffic homogeneity in the three different segments. For simplicity, the traffic matrixes were assumed identical for each network segment. Table 1 includes the traffic matrix for one of these segments, the one composed by server 1 and routers 2, 3, 6 and 10.

Table 1 Traffic matrix in Mbps: a) data traffic, b) voice traffic, c) video traffic

	Server 1	*Router 2*	*Router 3*	*Router 6*	*Router 10*
Server 1	-	253.8	222.7	71.8	4.8
Router 2	99.4	-	19.4	2.4	-
Router 3	70.2	29.8	-	11.1	-
Router 6	51.2	10.1	10.8	-	-
Router 10	48.8	4.1	-	4.1	-

(a)

	Server 1	*Router 2*	*Router 3*	*Router 6*	*Router 10*
Server 1	-	34.5	-	34.5	-
Router 2	73.9	-	-	38.1	-
Router 3	-	-	-	-	-
Router 6	17.2	8.9	-	-	-
Router 10	-	-	-	-	-

(b)

	Server 1	*Router 2*	*Router 3*	*Router 6*	*Router 10*
Server 1	-	-	(*) VTx0.66	(*) VTx0.34	-
Router 2	-	-	-	-	-
Router 3	15	-	-	-	-
Router 6	17.5	-	-	-	-
Router 10	-	-	-	-	-

(*) Concerning the video traffic (VT) generated by the Servers (Servers 1, 2 and 3), we considered four different cases:
VT = 0 (No video service)
VT = 0.33 Gbps
VT = 0.43 Gbps
VT = 0.83 Gbps

(c)

These traffic matrixes were obtained from the estimation of traffic flows on the above-mentioned realistic environment (Milan city). Such an estimation was carried out within the LION project [8] taking into account not only the characteristics of each service, but also the penetration (percentage of customers) of such kind of services.

Concerning the traffic model, for data traffic sources we used the ON-OFF with burstiness (peak rate/average rate) b = 10, and mean burst length BL = 10 packet times and for voice and video traffic sources, we used Poisson model with a mean packet arrival of λ packets per second. For data traffic, we considered the IP packet size statistical distribution given in [10], while for voice and video packets we used fixed packet size, 44 bytes and 512 bytes respectively.

We carried out two sets of simulations, one considering a link failure and the other considering a node failure, in such a way that the failure is produced at certain instant of the simulations (t = 70 ms), either a fibre cut between two routers not directly connected to the server, or a node (router) failure. One of the routers, missing the reception of control packets, detects the failure, and starts the recovery process. Figure 7 depicts the simulated failure scenarios, Figure 7-a the link failure case and Figure 7-b the node failure case.

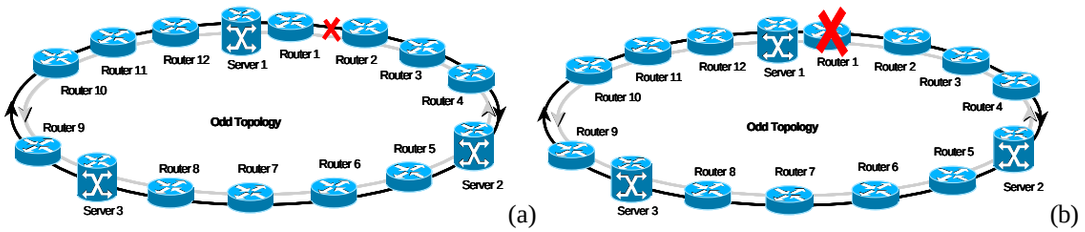


Figure 7 Simulated failure scenarios

The simulated time was 300 ms for the case of node failure and 200 ms for the case of link failure.

4.2. Experiments and Results

This Section includes a sample of the results obtained for the above described simulation scenario. All the results reported concern to the case where the video serves generate in average VT = 0.33 Gbps each, and focus in the evolution of the throughput during the simulation.

Figure 8-a plots the throughput as a function of the operation time simulated (200 ms) in case of a link failure (as shown in Figure 7-a). The initial oscillation corresponds to the simulation transient time. At t = 0.07 s we force a fibre cut described above. Due to the failure, the throughput begins to decrease (network cannot serve all the traffic and some packet losses occur). After the wrapping, the network stops to loose traffic and the topology discovery protocols starts to work in order to find the right direction to send the traffic through the new shortest paths. Once the topology map is updated at all nodes, the SRP-fa algorithm needs some time to stabilize. As is indicated in the figure, the total time we estimated for a full recovery after the failure (network reaches again the stable situation) is 40 ms. Furthermore, it is difficult to estimate from the figure, but from the simulation results we estimated that the time needed to restore the traffic from the link failure is less than 2 ms, while the time needed by the TD protocol to update the nodes topology databases is less than 1 ms. During the failure around 600 packets were lost, 15% of them of HP traffic. Other interesting result provided by the simulation results is that after reaching again the stability, the average end-to-end delay suffered a significant increase, in particular, a 50% for the HP traffic.

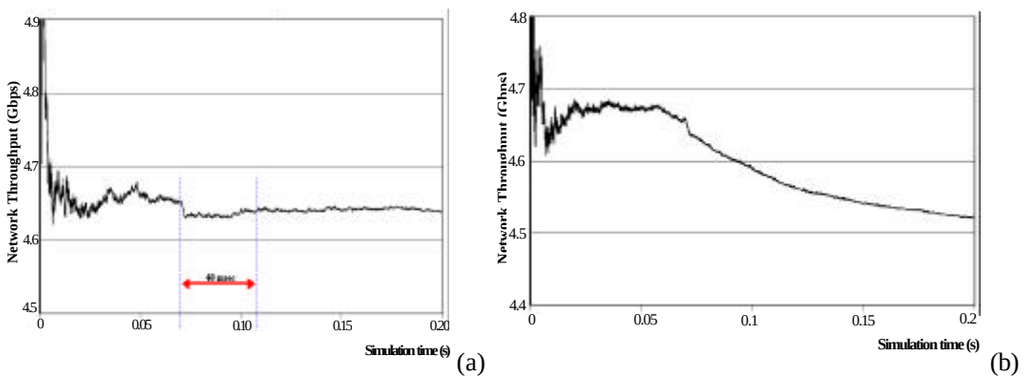


Figure 8 Network throughput evolution after a fibre cut failure, a) for the whole network (see Figure 7-a), b) for a single segment (1 Server plus 4 routers)

Figure 8-b reports the network throughput evolution for a variant of the above-described simulation scenario, which consisting of concentrate the whole traffic in a single segment and reconfiguring this

segment as a physical disjoint DPT network. This leads to a DPT ring composed by five nodes (one server and four routers), handling three times more traffic than a segment of the original configuration (values of the traffic matrix included in Table 1 have tone multiplied by 3). The simulations results obtained in this case indicate that both IPS and TD protocols worked properly, the time spent by the IPS protocol to restore the ring from the failure was less than 2 ms, while to update the nodes topology databases the TD protocol needed less than 1 ms. Nevertheless, due to the wrapping, the available bandwidth decreased, which lead to a saturation of the network, SRP-fa did not reach a stable situation again. It is worth noting that in this case (did not happen the same in other the other cases simulated) the saturation affected only the LO priority traffic (end-to-to end delay growth to infinite), HP traffic suffered an strong increase of the end-to end delay, but could continue being served

To summarize, Figure 8-a shows that the IPS protocol achieves a very good performance, since the time the network lasted from the failure to come back again to the steady state is (~40 ms) less than 50 ms, the typical restoration time of APS in SONET/SDH networks; and Figure 8-b shows that under heavy load conditions, IPS also works properly, but after recovering from the failure the network may become saturated (may not reach a steady state). In the simulations under heavy load conditions (VT = 0.43 Gbps and VT = 0.83 Gbps), the network became saturated after recovering from the fibre cut failure

Again for the initial network (3 segments and VT per server = 0.33 Gbps), Figure 9-a plots the throughput as a function of the operation time simulated (300 ms) in case of a node failure (as shown in Figure 7-b). Note that after the node failure, the throughput decreases and seems not to reach a stable situation, but this is not really true. It reaches the stability, but it takes long (> 200 ms) and the final throughput is lower than before the failure. This is due to the fact that after the failure the node that failed does not inject traffic in the ring anymore, and the rest of nodes, once they know that there is a node exluded from the network (thanks to the TD procedure) stop sending traffic towards that node. Figure 9-a obtained in the case of no video service (VT per server = 0), confirms this behaviour, the network throughput evolves towards a steady state after the stabilization of the SRP-fa algorithm and the DPT ring remains working efficiently. We estimated that the necessary time to come back to stability, in this case was 70 ms.

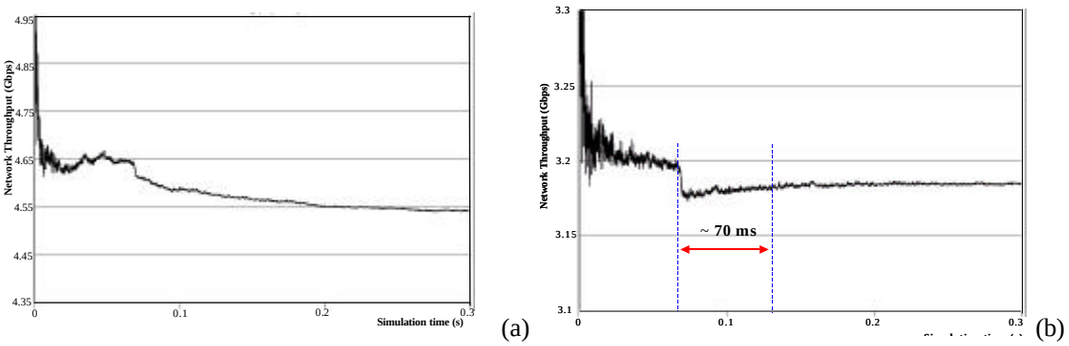


Figure 9 Network throughput evolution after a node failure, a) Average video traffic generated by the servers VT = 0.33 Gbps, b) no video traffic generated by the servers

Figure 9 show that also in case of node failures, IPS and the TD protocols conform their role. The former by the ring wrapping, and notifying the failure to the rest of nodes. The latter excluding the node that failed from the ring. Both protocols took less than 2 ms to recovery the ring. Nevertheless the SRP-fa stabilization took longer than in the case of a fibre cut. Furthermore, like in the case of fibre cuts, in the simulations under heavy load conditions (VT = 0.43 Gbps and VT = 0.83 Gbps), the network became saturated after recovering from the node failure.

5. Simulation Studies: Case study 2

This case study was carried out using *ns* simulator and considering the special traffic assignments defined previously in Section 3. Recall that the motivation for defining and investigating analytically 3 special cases was to show unexpected behaviour of DPT (RPR) ring carrying LO traffic and throttling of traffic streams due to traffic overlapping. For HI traffic, a kind of admission control and bandwidth management seems to be necessary in order to fulfil client's requirements, before and after wrapping.

5.1. Simulation scenario

The behaviour of 8-node RPR ring with traffic same as for case 2 (see Figure 4) will be presented. External ring carries traffic in clockwise direction, internal ring in counter-clockwise direction, all spans have same capacity 622 Mbps. Time interval between sending subsequent Topology Discovery packets is equal to 0.2 s, propagation delay is 0,1 ms (100μs, 20km span length) packet size 402 B and each node sends UDP traffic with maximum speed (greedy applications). Since buffer parameters (SRP-fa parameters) have significant impact on transport, they were chosen according to specific MAC proposal: Low Priority Transit Buffer - 750 packets, LOW_THRESHOLD - 187 packets (25%) and HIGH_ THRESHOLD - 749 packets.

There were following simulated events: t = 0 – start of simulation run; t = 0,15 s – link failure (2 → 3), recognised by node 3; and t = 0,70 s – end of simulation.

5.2. Experiments and Results

Case 2 (Section 3) depicts situation with very inefficient traffic assignment (after single failure of RPR element) and such situation should be avoided in operator's practice. Figure 4 shows traffic streams sent before (left side) and after single link failure occurring between nodes 2 and 3. Below there are only sample results shown, proving that traffic behaviour predicted by theoretical investigations is generally valid, except for transient periods when some fluctuations occur.

Figure 10-a shows link occupancy between node 0 and 1. Before failure this link conveys one stream 0→3, sharing its bandwidth by SRP-fa with two other streams, 1→3 and 2→3 (dark solid line in Figure 5. Just after failure all streams are wrapped in node 2 and send to node 3 via whole ring. Since bandwidth is shared among 4 streams using SRP-fa mechanism, and 3 flows are sent via 1→0 span (light solid line in Figure 10-a), approximately 75% of span capacity is used. At time instant 0.35s, topology discovery recognises new situation and traffic streams 0→3, 2→3 1→3 and 2→3 are sent directly to node 3, without wrapping in node 2. Light solid line shows that capacity of span 0→1 is used at the level of 50 %.

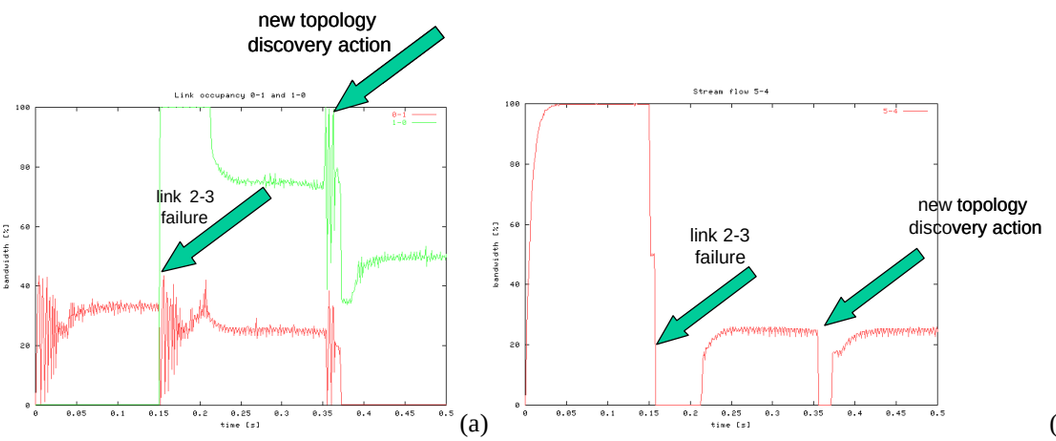


Figure 10 a) Illustration of link occupancies 0 -> 1 and 1 -> 0 for Case 2 (failure and topology discovery actions were simulated). b) Illustration of traffic streams 5-4 (significant reduction of available bandwidth)

Figure 10-b shows behaviour of single traffic stream 5→ 4. Before failure it uses whole capacity of span 5→ 4, after failure and also after topology discovery, this stream shares bandwidth with wrapped streams, so it gets 25 % of span capacity. Another important phenomenon is throttling of traffic at instants of failure and topology discovery reconfiguration due to sending excessive transit traffic from buffers (after wrapping and then switching back to primary routes due to topology discovery action).

6. Conclusions

In some cases DPT can show unexpected behaviour since support of LO/HI priority traffic streams, after failure and wrapping of rings, can be very complex and cause deadly reduction of capacity for LO traffic. Also, it is advisable to keep total HP traffic below 50% of the capacity in order not to jeopardize the behaviour of vital (real-time) services. DPT seems to be quite a good solution for transport of best effort traffic for slightly loaded networks.

In terms of recovering time, the simulation results obtained show that IPS has been optimised to wrap up the ring in the shortest possible time and thus to minimize the packets lost. Anyway, in DPT layer, after the ring wraps, the available bandwidth is lowered. A reoptimisation of the bandwidth utilization is needed and low priority traffic has to be re-converged fairly to the lowered bandwidth dynamically by using SRP-fa. Thus, the evaluation of the DPT performance in case of failure does not comprise only wrapping of the ring but also the stabilization of the connectivity available for higher layers.

Simulation results have shown importance of cases suggested by theoretical investigations (presented in Section 3). One can observe that in transient states there are not convenient phenomena related to switching of traffic (packets) at instants of failure and topology discovery reconfiguration due to sending excessive transit traffic from buffers.

DPT has no dedicated spare resources so each failure has to cause loss of traffic in a case of high load sent over the network. The idea of properly using DPT is generally idea of over provisioning of resources. The very basic assumption of running DPT ring without central management node (or CAC node) could be thus questioned.

DPT (RPR) is an optical ring technology, which provides fair bandwidth allocation among traffic streams (low priority traffic) with protection against any single failure. However, one should be aware of the following, counter-intuitive, behaviour: 1) After the failure the available bandwidth is reduced. The reduction factor depends on the actual load and distribution of traffic, the worst case value is about 94%. 2) After the recovery action in DPT (RPR) is completed one should expect two congestion events, which affect the traffic streams that were not affected by the failure itself. The first congestion lasts about 50ms and occurs right after the ring wrap, the second congestion is shorter and occurs after the topology discovery process is completed (approx. 200 ms. after the ring wrap). During the congestion the traffic flow may be completely blocked in the affected traffic streams.

7. References

[1] “Dynamic Packet Transport Technology and Performance”, Cisco System White paper, 2000.

[2] D. Tsiang, G. Suwala, RFC 2892, “The Cisco SRP MAC Layer Protocol”, August 2000.

[3] J. Moyano, S. Spadaro, J. Solé-Pareta, B. Bostica, “Performance Evaluation of SRP-fa algorithm used in DPT networks”, Proceedings of International Conference on Telecommunications ICT, Bucarest, Romania, 4-7 June 2001.

[4] “Dynamic Packet Transport Technology and Applications Overview”, Cisco System White paper, 1999.

[5] T. Brown, K. Tesink, RFC-1595, “Definitions of Managed Objects for the SONET/SDH Interface Type,” March 1994.

[6] S. Gjessing, “RPR’s worst case scenario”, (http://www.ieee802.org/17/documents/presentations/ jul2002/sg_worst_02.pdf).

[7] R. Lindemayer, “Provisioning in RPR networks”, (http://www.ieee802.org/17/documents/ presentations/jul2002/ rl_prov_02.pdf).

[8] Official LION Web site: http://www.telecom.ntua.gr/lion/.

[9] A. Jajszczyk, A. Szymanski, K. Wajda: “Issues of DPT efficiency in various traffic conditions”, 8th Polish Teletraffic Symposium, Zakopane, 3-5 September 2001.

[10] P. Lagner, “SDL Data Link Specification,” Lucent Technologies – White Paper, 1998.