

Flow-aware resilient ring: new proposal for metropolitan area networks

Jerzy Domżał¹

Published online: 14 May 2015

© The Author(s) 2015. This article is published with open access at Springerlink.com

Abstract The Flow-Aware Resilient Ring (FARR) as a new proposal for Metropolitan Area Networks is presented and analyzed in this paper. This new solution combines the best features of two known network architectures: Flow-Aware Networking and Resilient Packet Ring. Traffic in FARR networks is served as flows and implicitly classified into one of two classes: streaming (with high priority) or elastic (without priority but with assured bandwidth). This allows for providing Quality of Service guarantees in accordance with network neutrality rules. Moreover, high priority traffic is protected in case of a network element failure by the steering mechanism, which ensures fast traffic redirection in time less than 50 ms. The advantages and weaknesses of the proposed architecture are presented along with an analysis of traffic distribution in different topologies. The formulae provided in the paper allow a decision to be made on whether it is profitable to reconfigure a single-ring into a multi-ring topology. Moreover, it is shown that simultaneous implementation of FARR networks with congestion control mechanisms ensures fast, scalable and reliable transmission of streaming flows.

Keywords Flow-Aware Networks · Resilient Packet Ring · Quality of Service · Congestion control · Reliability

1 Introduction

Internet traffic grows rapidly every year. The structure of the Internet is changing. Next generation access architec-

tures like Fibre to the Building (FTTB) or Fibre to the Home (FTTH) are becoming increasingly popular. As a result, Internet traffic is growing rapidly. Many analyses show that it will grow significantly over the coming years. Lawrence Roberts, one of the founders of the Internet, predicts that network operators will have to serve double the traffic every year. Minnesota Internet Traffic Studies (MINTS) or Cisco foresee annual Internet traffic growth as approximately 40–60%. As a result, new quality of service solutions will be deeply desirable in the Future Internet, especially in the core. Modern Metropolitan Area Networks (MANs) have to be fast, resilient and consistent with net neutrality concept. The legal conditions of the net neutrality are discussed all over the world, including the United States Congress. Probably, in the final solution to the net neutrality problem, Internet Service Providers (ISPs) and operators will be able to differentiate the quality of Internet traffic. However, discrimination among traffic of the same type, e.g., generated by different users or applications will be forbidden [1]. There are many well known MAN architectures, e.g., SONET/SDH or Gigabit Ethernet, and other proposals designed and developed in the framework of European Union projects such as WONDER [2] and SWRON, or OPSRN studied in [3,4]. While the aforementioned architectures have many advantages, there are also some problems still to be solved. For example, SONET/SDH networks were designed for carrier-class performance and reliability, and for circuit-switched operation. As a result, they provide capacity for alternative routing when a network element fails [5]. However, network elements are quite complex and expensive. Moreover, in many cases resource utilization in SONET/SDH networks is inefficient. On the other hand, new proposals developed in many projects still require a great deal of research. Gigabit Ethernet or 10 Gigabit Ethernet are currently used in metro networks; however, they do not provide fairness or QoS guarantees.

✉ Jerzy Domżał
jdomzal@kt.agh.edu.pl

¹ Department of Telecommunications, AGH University of Science and Technology, Al. Mickiewicza 30, 30-059 Kraków, Poland

In this paper, a new solution called Flow-Aware Resilient Ring (FARR) is presented and analyzed. It was proposed in [6], where the results of the simulation experiments under congestion or a network element failure were presented. FARR combines the best features of Resilient Packet Ring (RPR) and Flow-Aware Networks (FAN). RPR is a well known architecture, standardized in 2004 and signed as IEEE 802.17 [7]. RPR is a technology that supports data transfer in a dual counter-rotating ring topology composed of up to 255 nodes. Generally RPR was designed as a universal technology that can be used in local, metropolitan and wide area networks. RPR's restoration mechanisms ensure automatic reaction to failures in a time of less than 50 ms, which is now a requirement for all networks [8]. FAN is quite a new networking architecture, which ensures quality of service (QoS) guarantees using only minimal knowledge from the network. This was proposed in [9] by Roberts and Oueslati. The complete architecture was presented in 2004 in [10]. In FAN, traffic is served as flows and implicitly classified into one of two types: elastic or streaming. This allows for providing QoS guarantees with respect to the net neutrality paradigms.

As a consequence, FARR ensures fast and reliable transmission in a dual optical ring architecture. It has been shown and proved by simulations that even in congestion or failure, priority traffic is protected. Moreover the key traffic, like voice over IP (VoIP) or video on demand (VoD) is sent with high priority in bigger topologies, too, e.g., composed of many FARR rings. The acceptance delay, QoS, and reliability of flows realizing VoIP or VoD connections are very important. To improve such transmissions, the method proposed in [11] may also be implemented in FARR. This assumes that the duplication of certain packets (e.g., VoIP or VoD) at edge routers may be used for better protection against failures, errors or packet losses.

The dual ring implementation used in FARR can easily be extended into architectures composed of many double counter-rotating rings connected by bridges or multi-functional nodes (inter-nodes). The idea behind such solutions is presented in Sect. 5. Multi-ring FARR networks, as well as providing congestion control and priority traffic protection under failure mechanisms, constitute a good proposal for MAN architecture to be used in the Future Internet. This paper extends the work presented in [6] with a more detailed description of the FARR architecture and new simulation results. However, the main contribution of the paper is the analytical analysis of bandwidth assignment for flows in single and multi-ring FARR architectures. As a result, the closed-form expressions presented in the paper may be used by network administrators to plan a network topology in the best possible way. All three parts of the paper give the reader a common view of the analyzed architectures, show how FARR works and explain the advantages of using multi-ring architectures. To understand the theoretical analysis presented in

Sect. 5, the reader should be aware of how FARR networks work and what is needed to improve the performance of streaming flows in a FARR architecture.

This paper is organized as follows. Section 2 describes the RPR and FAN concepts. Section 3 shows the assumptions and the description of the new FARR proposal. In Sect. 4, the FARR simulation analysis is presented. The analysis of the fairness algorithm used in FARR and bandwidth assignment in single-ring and multi-ring topologies is provided in Sect. 5. Section 6 concludes the paper.

2 RPR and FAN basics

FARR is a combination of RPR and FAN. In this section, the basics of these two architectures are presented.

2.1 Resilient Packet Ring

RPR is one of the newest protocols for MANs standardized by IEEE (IEEE 802.17). It is based on the Dynamic Packet Transport (DPT) concept proposed by Cisco in 2000 for use in optical fibre ring networks [12, 13]. RPR inherits the advantages of DPT and extends and improves its functionality. The main features of RPR are as follows:

- two protection mechanisms (steering and wrapping),
- interoperability with major transmission standards,
- scalability in speeds and number of nodes,
- spatial reuse possibility,
- possible performance monitoring,
- built-in fault isolation feature,
- support for a limited number of priorities (2 or 3).

The RPR architecture is based on two symmetric, counter rotating rings. One of them is called *inner* and the second *outer*. Packets are transmitted in both rings simultaneously in opposite directions. When data packets are transmitted in the outer ring, the corresponding control packets are sent in the inner ring. Packets are stripped at the destination nodes, which allows provision of the spatial reuse mechanism. As a result, packets may be transmitted in different parts of the network without sharing the available bandwidth. The maximum number of nodes in RPR rings is 255 and its maximum circumference should be less than 2000 km. The protocol is designed to operate over a variety of physical layers, including SONET/SDH, Gigabit Ethernet (IEEE 802.3ab), DWDM and dark fibre. It is expected that RPR will be able to work over higher-speed physical layers. The minimum supported data rate is 155 Mb/s. RPR networks complement other architectures, e.g., IEEE 802.3. Moreover, the ring topologies are easily addressed and support unicast, multicast and broadcast data transfers [7].

The topology discovery (TD) mechanism used in RPR networks allows for fast and automatic recognition of any type of topology change. It is activated when an RPR network is created, and each time a node or link fails or topology changes (e.g., when a node is added to the ring or removed). Moreover, TD packets are also sent periodically to ensure proper topology map distribution. Data transmission in RPR networks is possible if each node receives TD packets and, based on them, builds the topology map.

RPR supports three traffic classes:

- *class A* high priority traffic which has an absolute priority over low priority traffic; designed for real time services with low delays and guaranteed link bandwidth demands, e.g., VoD,
- *class B* medium priority traffic for which a contract is needed; the “in-contract” part of medium priority traffic is treated as high priority traffic, e.g., VoIP, while the out-of-contract part of traffic is sent as low priority traffic or dropped,
- *class C* low priority traffic shaped in RPR nodes to achieve fairness among competing traffic streams; designed for the best effort traffic, e.g., data transfers.

The fairness algorithm is implemented to ensure efficient bandwidth allocation. It is used for low and medium priority traffic (classes B and C respectively). All available bandwidth is shared fairly between nodes sending data.

One of the main advantages of RPR is its rapid reaction to any network element failure. There are two mechanisms which may be activated after failure:

- *steering protection* an obligatory mechanism implemented in each node; after failure packets are redirected in the source node to the opposite ring in order to avoid sending them via failed links or nodes,
- *wrapping protection* activated only in nodes which have declared it during the TD process; after failure, packets are redirected via a node located next to the failed link or node and sent in the other ring.

The above TD mechanisms ensure fast reaction to any failure. As a result, a transmission break in any flow is always shorter than 50 ms.

2.2 Flow-Aware Networks

FAN were proposed to enable the proper quality of service (QoS) for flows in an implicit way and using only minimal knowledge of the network. By flow we mean all packets which are transmitted from one source node to a fixed destination and which use specific port numbers and transmission protocol. There are two flow types proposed for FAN:

- *elastic* usually used for data transmission, served with the best effort regime,
- *streaming* used for low bandwidth consuming services, e.g., VoIP calls, served with priority over the elastic type.

All the flows are classified into one of the above types based on queue occupation and, then, served with (streaming) or without (elastic) priority. No packet labels are needed or expected. This way, services in a network may be differentiated implicitly. Moreover, the fairness between elastic flows is maintained. The features presented above mean that FAN differs from well known QoS architectures like Differentiated Services (DiffServ) [14] or Integrated Services (IntServ) [15]. In particular, FAN is easier to implement and, thanks to implicit flow differentiation, easily conforms to net neutrality paradigms. However, in [16] a new methodology for providing statistical guarantees within the DiffServ model in a network was proposed. In this solution, a utilization-based admission control scheme was employed for implicit flow admission. As an effect, an explicit delay computation at admission is not necessary and the system utilization in this case is much higher than in original DiffServ. Based on this example, we may observe how important implicit flow identification is.

The flows in FAN are served in cross-protect routers (also denoted as XP’s), which are the basic elements of this architecture [10]. The model of the cross-protect router is shown in Fig. 1.

The main elements of cross-protect routers are: the admission control block (AC), which decides whether to accept or reject packets of flows, and the scheduler, which is responsible for packet queuing and periodic measuring the values of the following two parameters:

- *fair_rate* estimates the maximum rate that might be or is realized by elastic flows,
- *priority_load* measured as a quotient of the sum of the queued packet lengths (with priority) in a given time period to the length of this period.

In the congestion-less state, new flows are accepted in the AC block and their identifiers (IDs) are written to the Protected Flow List (PFL). The ID of a flow is removed from the PFL if the flow is inactive for a fixed time period given by the value of the *pfl_flow_timeout* parameter. Each outgoing link connected to the FAN router has its own PFL. On the other hand, in congestion, only packets of flows whose IDs are on the PFL are accepted and served. This means that sometimes a new flow has to wait a long time before it is allowed to begin transmission. This situation is unacceptable for real-time applications like voice over IP (VoIP) or video on demand (VoD). For example, the setup time (post-selection delay) of local VoIP calls should be less than 6 s

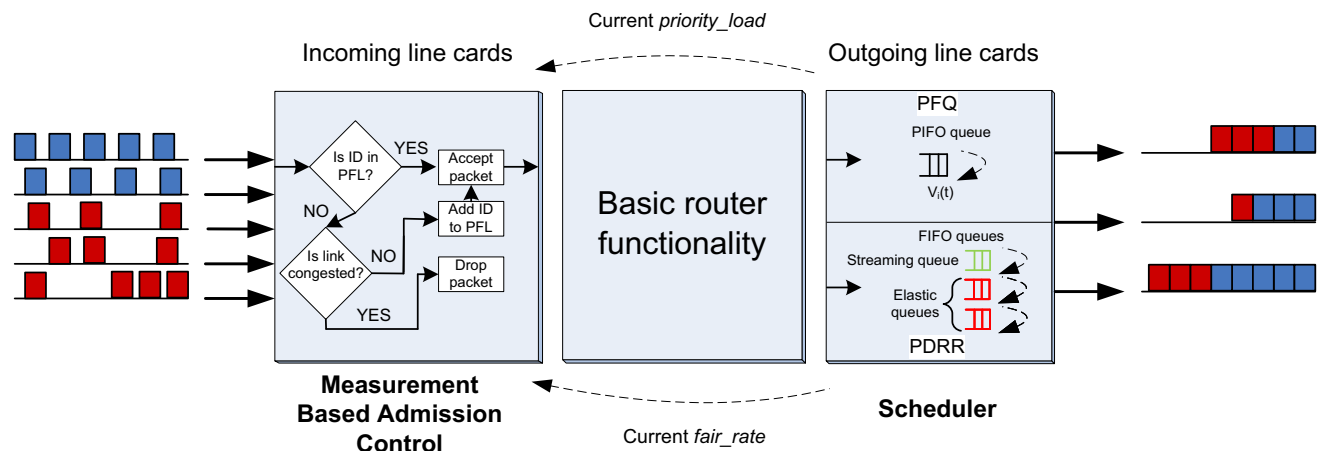


Fig. 1 The cross-protect router architecture

while for international calls it should not exceed 11 s [17]. The congestion state is observed if the value of *fair_rate* is lower than the *min_fair_rate* (minimum allowed value of the *fair_rate*) or the value of *priority_load* is higher than the *max_priority_load* (maximum allowed value of the *priority_load*).

Two scheduling algorithms were proposed for use in FAN: Priority Fair Queuing (PFQ) [10] or Priority Deficit Round Robin (PDRR) [18]. There is also a new proposal, called Approximate Flow-Aware Networking (AFAN), which assumes the use of the Approximate Fair Dropping (AFD) algorithm for scheduling packets [19]. The simulation analysis presented in this paper is provided only for the PFQ algorithm. The results of the same analysis for FAN with the PDRR or AFAN are similar to those obtained for FAN with the PFQ.

One of the most important advantages of FAN is its scalability. The complexity of queuing algorithms does not increase with the link capacity because the number of active flows is almost stable. This has been shown in [20]. Fair queuing is feasible, as long as link load is not allowed to attain saturation levels, which is asserted by the admission control. Compared to other QoS architectures, due to the lack of signalling and very low data handling complexity, scalability is achieved for FAN and not matched by any other architecture [21].

3 Flow-Aware Resilient Ring

RPR is a well known standard implemented in many countries, e.g., USA or China. It is still considered to be one of the promising architectures for the Future Internet [22]. However, while it is a stable solution, certain improvements are still required. One of the most important problems associated with RPR is traffic classification. It is not clear how

to distinguish packets and assign them to the proper traffic class. One of the possible solutions is to use the DS field in the header of an IP packet. In IPv4 it is the Type of Service (ToS) byte while in IPv6 it is the Traffic Class (TC) byte. Such a concept has some known drawbacks. For example, malicious users may try to change the values of the DS field to speed up their transmission. Moreover, the explicit traffic classification may not be consistent with the network neutrality concept. The idea of net neutrality is that a user's traffic is not discriminated at all in relation to traffic generated by other network users. This means that packets of similar applications (e.g., realizing VoIP connections) have to be served alike. In the most rigorous concept of net neutrality, all incoming traffic is sent as a best effort service and the ISPs cannot introduce any kind of traffic discrimination. On the other hand, in the most probable concept for net neutrality, traffic may be served with explicit classifications, but ISPs are not allowed to promote/degrade traffic within the same class. However, in the most promising solutions from the net neutrality point of view, traffic is sent in different ways based on implicit classification (without ISPs interference). This means that the values written to the DS field are ignored by routers connected to the source nodes. One of the most important advantages of RPR is its reliability [23]. Protection and TD mechanisms ensure fast traffic redirection in time less than 50 ms.

The problems presented for RPR networks are not observed in FAN, where traffic is implicitly classified and it is not possible to force special treatment of traffic from cross-protect routers. High priority traffic is identified based only on traffic characteristics and served first in the routers. It ensures conformity with each version of the net neutrality concept. While FAN works well under normal conditions, there are still some problems which have to be solved when considering reliable transmission. For a network element failure, traffic usually needs to be redirected to another route. As

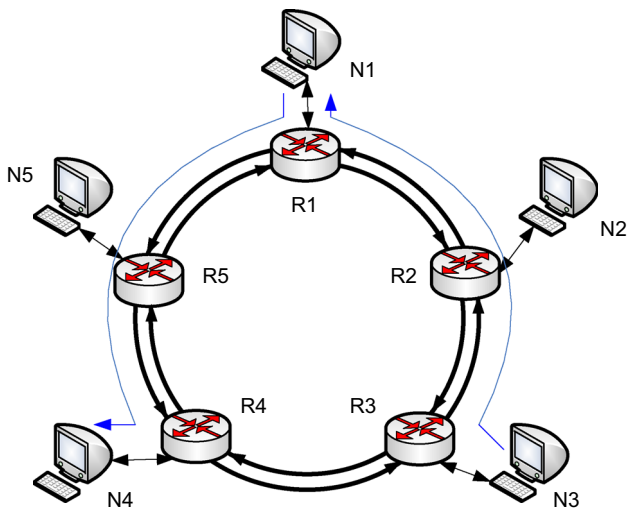


Fig. 2 Reference topology of FARR network

shown in [24], if traffic is redirected to a congested link not all streaming flows are re-accepted in a short time, which is very unfavourable for users making phone calls or participating in a video conference. On the other hand, if traffic is redirected to a congestion-less link, too many flows may be accepted at once and the transmission parameters deteriorate. There are several proposals which present solutions to the lack of resources problems in FAN. In [25], multi-layer FAN/WDM cooperation is assumed and analyzed. It is shown that it is possible to deal with a failure in the optical domain only if there are enough resources. If this is impossible, traffic needs to be redirected in the IP layer. Paper [26] presents the concept of Global Protected Flow List (GPFL), which in some cases ensures fast redirection. The authors of [27] suggest that excessive traffic which cannot be accepted in XP routers may be sent directly using the optical domain. In each of these solutions, significant effort is needed to ensure a prompt, correct reaction to a failure.

The FARR presented in this paper combines the advantages of both architectures described above. In FARR we assume the ring topology. The neighbour nodes are connected by two single one-way links (in opposite directions). The routers are cross-protected. As packets are destination stripped, spatial reuse is allowed. The traffic is sent as flows (elastic or streaming) without any packet marking and signalling. The TD protocol is implemented to ensure the proper behaviour of protection mechanisms (steering or wrapping). The streaming flows are sent with priority, and fairness among elastic flows is guaranteed by implementing the scheduling algorithm. Flows classification is implicit, as in FAN.

An example of the FARR network composed of five nodes is presented in Fig. 2. The topology shown in this figure was the reference version in the simulation experiments.

4 Simulation analysis of FARR network

The simulation analysis presented in this section has been provided to show how FARR networks operate. In the first experiment, the acceptance time for the streaming flows in the congested FARR network was observed.

50 simulation runs were conducted in variety of situations. The duration of each simulation run was set to 500 s to observe the acceptance times for streaming flows in each router on their routes. The number of background elastic flows activated by each node was changed ranging from 200 to 600 and were generated following the Pareto distribution (shape factor = 1.5, mean size = 150 Mb). The elastic flows were sent as follows: from N1 to N4, from N2 to N5, from N3 to N1, from N4 to N2, and from N5 to N3. This assignment meant that all elastic traffic was sent through the outer ring and each link in this ring was congested from the beginning of the simulation experiment. The exponential distribution for generating the time intervals between the starting points of transmissions of elastic flows (with mean interarrival time = 0.1 s), as well as for generating the start times of streaming flows (with mean interarrival time = 1 s) was used. 20 streaming flows were sent from node N3 to N1 and other 20 streaming flows were sent from node N1 to N4 (see Fig. 2). In both cases, traffic was sent through the outer link based on the information from the TD protocol. The VoIP connections realizing the Skype service were analyzed. The packet size was set to 100 bytes and the transmission rate was set to 80 kbit/s for each of the streaming flows. The elastic traffic was treated as background traffic and used to saturate the analyzed links. It was assumed that the capacity of links between routers was set to 100 M/s and the PFQ algorithm was implemented. The capacity of access links (with FIFO queues) was set to 1 Gb/s. The buffers in XP routers were sized to 1000 packets, which is a reasonable value for FARR links, and the MTU was set to 1500 bytes. The measurement interval for the *priority_load* parameter was set to 50 ms while the *fair_rate* values were estimated every 500 ms. The *max_priority_load* and the *min_fair_rate* were set to 70 and 5 % of the link capacity, respectively, and the *pfl_flow_timeout* parameter was set to 20 s, which is the time after which an ID of inactive flow is removed from the PFL. Each experiment was repeated 10 times in the same conditions to ensure statistical credibility. 95 % confidence intervals were calculated by using the Student's t-distribution.

The mean values for *waiting_time* (acceptance time of streaming flows) in each router on their routes are presented in Table 1.

The results show that streaming flows are accepted after tens of seconds in the first routers on their routes (R3 for flows sent from N3 to N1 and R1 for flows sent from N1 to N4) and after about a hundred seconds in the second routers (R2 for flows sent from N3 to N1 and R5 for flows sent

Table 1 The *waiting_time* values of streaming flows in routers

No.	R1 (s)	R5 (s)	R3 (s)	R2 (s)
200	53.42 ± 33.72	97.17 ± 39.74	92.56 ± 49.34	132.61 ± 77.04
300	64.24 ± 31.54	107.96 ± 25.88	87.36 ± 64.39	135.17 ± 73.35
400	48.05 ± 37.12	93.57 ± 32.24	85.37 ± 60.30	132.62 ± 60.41
500	43.82 ± 18.76	90.92 ± 21.73	71.98 ± 38.13	133.84 ± 44.79
600	66.18 ± 35.89	101.12 ± 29.35	96.43 ± 62.60	141.82 ± 63.72

from N1 to N4). This means that a user usually has to wait over 100 s before his/her call is set. This time is completely unacceptable. We have to note that, according to [17], the setup time (post-selection delay) of local calls should be less than 6 s, while for international calls it should not exceed 11 s. The acceptance times from streaming flows are long because the accepted elastic flows have to send a large volume of traffic (mean size of traffic for an elastic flow was set to 150 Mb) and until at least some of them finish, access to the router is blocked. The second conclusion is that acceptance times for streaming flows do not depend on the number of elastic flows active in the background, but on the volume of traffic to be sent by accepted elastic flows. Therefore, for simplicity, in the following experiments, a constant value (200) of elastic flows sent by each node was assumed.

The problem of long acceptance times for streaming flows in FARR networks may be solved by congestion control mechanisms. The most promising one, called RPAEF (Remove and Prioritize in access Active Elastic Flows) is described and analyzed in the following section.

4.1 The RPAEF and limiting mechanism

Several congestion control mechanisms have been proposed for FAN [28], e.g., Enhanced Flushing Mechanism (EFM), Remove Active Elastic Flows (RAEF), Remove and Block Active Elastic Flows (RBAEF), and Remove and Prioritize in access Active Elastic Flows (RPAEF). All these mechanisms work based on partial or total periodical cleaning of the PFL content in congestion. The goal is to ensure that streaming flows are accepted in a sufficiently short time. The RPAEF mechanism looks to be one of the most promising solutions for FAN (and also for FARR) and, therefore, it is presented and analyzed in detail. This algorithm was first presented in [26].

When a packet from a new flow arrives at a router in congestion, all IDs for flows being active for at least *active_time* are removed from the PFL and written to the Priority Access Flow List (PAFL) for a short time given by the *priority_access* parameter.

If a packet arriving at the admission control block in a congestion-less state belongs to the flow, the identifier of which is in the PAFL, the packet is always accepted. On

the other hand, packets of flows whose identifiers are not in the PAFL are accepted with low probability P_{RPAEF} (e.g., 0.03). The acceptance probability is set to 1 if PAFL is empty.

The idea of this solution is to ensure a short acceptance time for new streaming flows without breaks in transmission of elastic flows whose identifiers have been deleted from the PFL. The removed elastic flows are accepted again in the AC block immediately, while the rest of flows begin transmission with low probability P_{RPAEF} . Here, UDP flows with small packets (streaming flows) have a much greater chance of acceptance than TCP flows with bigger packets. Hence, streaming flows have precedence in acceptance over elastic ones.

Moreover, the proposed mechanism allows a decrease in the total number of all flows accepted after cleaning the PFL content in comparison to the other proposed solutions. It ensures that, once accepted, elastic flows have an opportunity to transmit their traffic with very short, harmless breaks and at an acceptable rate.

While the RPAEF mechanism ensures reasonable performance for streaming flows, there is still a need to decrease the number of elastic flows accepted in the routers after cleaning the PFL. If the number of elastic active flows is too great, it is not possible to serve them with a guaranteed minimum acceptable fair rate. To deal with this problem a limiting mechanism is proposed. The main goal of this solution is to limit to N the maximum number of accepted flows in the time period between any two consecutive measurements of the *fair_rate* parameter. The N parameter is estimated from the following formula:

$$\begin{cases} N = 100 / (\min_fair_rate \times i) & \text{if } i > 0 \\ N = \infty & \text{if } i = 0 \end{cases} \quad (1)$$

where $i \in \mathbb{N}$ is the parameter which may be changed to obtain the proper value of N . For example, if i is set to 2 and the *min_fair_rate* is set to 5%, it means that up to 10 flows may be accepted in the router during one measurement period of *fair_rate*. This value of i was assumed in the following simulation experiments based on the results presented in [26].

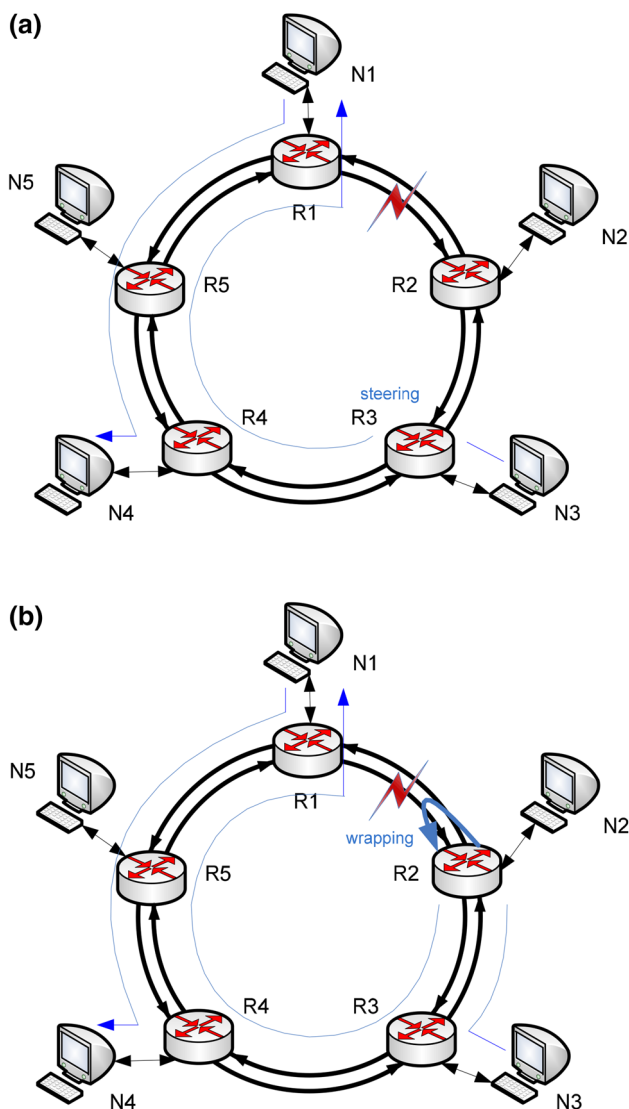


Fig. 3 FARR network: a failure repaired by steering mechanism, b failure repaired by wrapping mechanism

4.2 Simulation analysis of FARR with RPAEF and a limiting mechanism

The simulation experiment described in this section is illustrated in Fig. 3. 20 simulation experiments (10 with steering and 10 with wrapping) were conducted. The simulation parameters were exactly the same as in the previous experiment. It was only assumed that each node sends a constant number of elastic flows (200) and at 200 s the links between routers R1 and R2 fail. Moreover, an additional 200 elastic flows from node N3 to node N5 were generated. This ensured that inner links between routers R3 and R5 were congested. Two cases were considered: the failure was repaired by the steering (Fig. 3a) or wrapping (Fig. 3b) mechanism. We can see that the wrapping mechanism lengthens the route after fail-

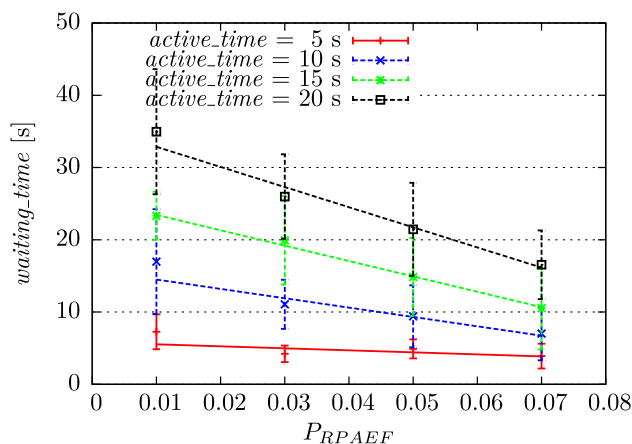


Fig. 4 Acceptance times of streaming flows in FARR with RPAEF and limiting mechanism

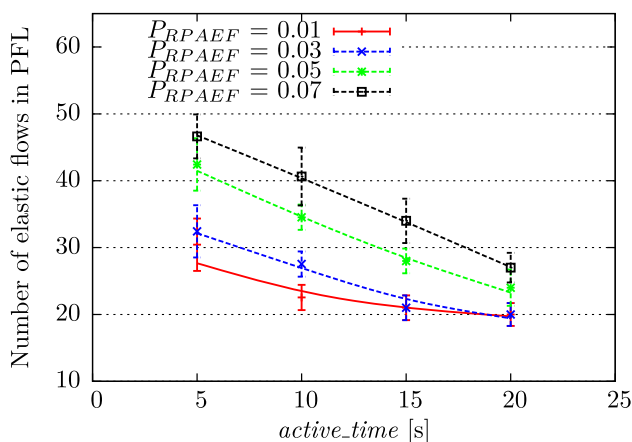


Fig. 5 Number of elastic flows accepted in the PFL in FARR with RPAEF and limiting mechanism

ure in comparison to the steering solution. This increases the acceptance time of redirected flows. The steering mechanism is considered the better one. That is why the results of the simulation experiments are presented for the case from Fig. 3a.

Analysis was conducted for different values of the *active_time* parameter (5 s, 10 s, 15 s or 20 s) and P_{RPAEF} parameter (0.01, 0.03, 0.05 or 0.07). The results presented in Fig. 4 show the acceptance times for streaming flows sent by node N3 in router R2 (before failure). We can see that the values of the *waiting_time* parameter decrease with the increasing values of the P_{RPAEF} values. Moreover, the values of the observed parameter also increase with increasing values of the *active_time* parameter, that is, when the IDs of elastic flows are removed from the PFL less frequently. We note that according to [17] accepted values (less than 6 s) are observed only for *active_time* = 5 s and $P_{RPAEF} \geq 0.03$.

The results presented in Fig. 5 show the mean number of elastic flows accepted in router R2 (before failure). We can

Table 2 The *waiting_time* values on a backup route of streaming flows

<i>waiting_time/i</i>	R3 (s)	R4 (s)	R5 (s)
–/–	231.20 ± 47.74	231.30 ± 47.70	236.82 ± 46.13
5/2	201.50 ± 1.04	202.05 ± 1.14	203.95 ± 2.05
10/2	202.25 ± 2.37	205.05 ± 6.58	209.95 ± 10.96

see that the values of the observed parameter decrease with increasing values of the *active_time* parameter and increase with increasing values of the P_{RPAEF} parameter. The analyzed values are best for $P_{RPAEF} = 0.01$ and insignificantly worse for $P_{RPAEF} = 0.03$.

Based on the results presented in this section we assume that $P_{RPAEF} = 0.03$ is the value to be used in the RPAEF mechanism for FARR networks.

The results presented in Table 2 show the mean acceptance times for redirected streaming flows after failure (at 200 s) in each router on their new route. We can see that if we do not use the RPAEF and limiting mechanisms (the first row in the table) the break in transmission is definitely too long. If we implement the RPAEF and limiting mechanisms (with $P_{RPAEF} = 0.03$ and $i = 2$) the outages in streaming flow transmission are reduced to a few seconds. While these values may be acceptable from the users point of view, the desirable solution should not cause any breaks at all. In the following section, a mechanism is presented which meets this requirement.

4.3 Global protected flow list in FARR

To improve network performance after failure in FARR networks, a GPFL may be used. The mechanism was proposed for FAN in [26]. The pseudocode for realizing the function-

ality of the GPFL in FARR networks is presented in Table 3. The global list should be implemented in each router. It contains the IDs of flows accepted on both links (in the inner and outer rings) connected to the router. Moreover, in GPFL there is also information on whether a flow is streaming or elastic. This condition is checked each time a packet arrives at the router based on the number of bytes queued at a time. If a packet of a new flow arrives in a congestion-less state, its ID is added to the PFL and GPFL. On the other hand, if a packet of a new flow arrives in a congestion state, it is accepted if its ID is in the GPFL and it is a streaming flow. This allows immediate acceptance of redirected streaming flows in a router operating on steering protection.

The DS field mentioned before in Sect. 3 is proposed to be used to mark the first packets of redirected streaming flows. It was assumed to set DS=0 in the header of each packet incoming from a source node (line 2). If a router sees that DS=1 then it knows that it is the first packet of a redirected streaming flow and accepts such a packet (lines 7–9). The DS field of a packet is set to 1 if this is the first packet of a redirected streaming flow (if a packet is accepted based on the GPFL criterion) (lines 10–11). Marking packets by using the DS field is carried out by FARR routers without interference from applications or network administrators. The mechanism is used only when a failure occurs in a network. Based on these assumptions, we may assume that violation of network neutrality paradigms is very difficult, but of course possible.

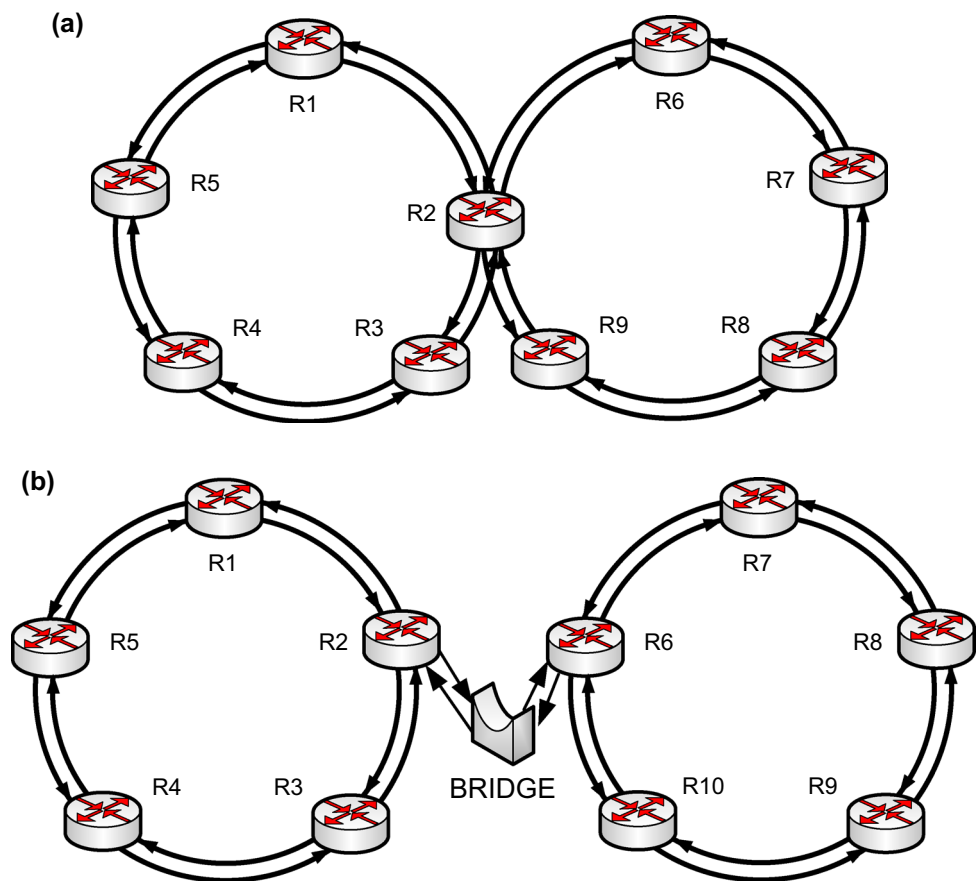
4.4 Simulation analysis of FARR with RPAEF, limiting mechanisms and GPFL

10 simulation runs were provided in the same conditions as in the previous experiment but with GPFL implemented. The simulation results show that the redirected streaming flows (under the control of the steering mechanism) were

Table 3 Pseudo code for realizing the GPFL functionality in FARR

1. on arriving packet p to the router in congestion
2. **If** p is a source packet **then** set DS=0 of packet p
3. **If** $flow_ID(p)$ is in the PFL of outgoing link **then**
4. accept packet p
5. **Else**
6. begin
7. **If** $flow_ID(p)$ is in the GPFL or DS=1 of packet p **then**
8. begin
9. add $flow_ID(p)$ to the PFL of outgoing link
10. **If** DS=0 of packet p **then**
11. set DS=1 of packet p
12. accept packet p
13. end
14. **Else** discard packet p
15. end

Fig. 6 Two possibilities for realization multi-ring architectures in FARR: **a** with inter-node, **b** with bridge



accepted immediately in each router on their new route and the performance of the network was achieved at an invariant level.

As we can see, the FARR networks with the RPAEF congestion control mechanism, the limiting mechanism and GPFL ensure fast and reliable transmission of streaming flows and fairness among elastic ones. In the following section, it is shown that this promising architecture may easily be extended from a single ring to multi-ring topologies. The analysis presented allows planning of a network topology in a way that meets user requirements and additionally improves transmission parameters for streaming flows.

5 Single and multi-ring topologies in FARR

The main motivation for considering multi-ring topologies for FARR networks is the opportunity to improve transmission flexibility and efficiency. In this paper, two possible implementations of multi-ring structures in FARR are investigated. The proposals are related to those identified for RPR. In the first solution, we have to implement a special node which is able to identify all the nodes in the rings it connects (Fig. 6a). The second possibility is to use bridges between rings (Fig. 6b). In this solution an additional MAC sublayer,

called a Spatially Aware Sublayer (SAS), is proposed to enable connections between nodes from different rings. This concept is similar to those proposed in the 802.17b standard for RPR [29] and enables broadening of the functionality and size of FARR networks.

SAS ensures that the spatial reuse method is used even if the destination address of a station is remote (located in another ring). The main operation of the SAS sublayer is to associate a remote address (and optionally VLAN identifier) with FARR station's MAC that provides an interface assigned to the specific client, identified by the remote address. Nodes with the SAS sublayer can use directional transmissions over the ring. To associate remote addresses and virtual identifiers (VIDs) with local FARR addresses, a learning process is proposed. It is similar to the TD mechanism used in a single-ring FARR. Of course the operation of both resilient mechanisms, steering and wrapping, is the same as in the one ring architecture.

In the following section, the analysis of bandwidth assignment for elastic traffic in single and two-ring topologies is provided. The main observation concerning the fairness algorithm is that bandwidth allocated to each stream passing through the same (observed) link is defined by link capacity available for elastic traffic divided by the number of elastic flows. This is a fair share of bandwidth.

In order to analyze and show the usefulness of multi-ring topologies for FARR networks, first an analysis of traffic assignment for a single ring network is presented. Then, in the next section, this is extended to a two-ring topology. For simplicity, it is assumed that only elastic traffic is transmitted in the network. In real networks, however, the capacity divided among elastic flows should be decreased by the part assigned to streaming flows.

5.1 Single-ring topology

For simplicity, in this analysis, it is assumed that each node in the ring sends one flow to each other one in the ring as fast as possible. The fairness algorithm used in FARR ensures high transmission efficiency and fair usage of resources. As a result, if two flows use the same link, they receive 50 % of available capacity.

The analysis begins with a simple ring structure with only 3 nodes. Each node sends traffic to 2 other nodes using one of two rings (the shortest path is chosen), thus the bandwidth of each flow is equal to 100 % of link capacity. Let us depict the number of flows sharing the bandwidth of a single link as N_x . For a FARR ring comprised of only 3 nodes, N_x is equal to 1. Generalizing, each flow will receive C/N_x capacity, where C is the capacity of the link (it is assumed that each link in the ring has capacity C) and the N_x index is computed as in defined in Theorem 1.

Theorem 1

$$N_x = \begin{cases} \frac{n^2-1}{8} & \text{if } n\text{-odd; for both ringlets} \\ \frac{n^2}{8} - \frac{n}{4} & \text{if } n\text{-even; for inner ringlet} \\ \frac{n^2}{8} + \frac{n}{4} & \text{if } n\text{-even; for outer ringlet} \end{cases} \quad (2)$$

where n is the number of nodes in the ring. It is important to note that, in the nominal situation (no failure, thus no steering or wrapping used), traffic stream is sent to the destination node using the ringlet with the lower number of hops. If the number of hops is the same in both directions (an even number of nodes), the output ringlet is chosen by default (as in RPR). Thus, in this case the input ringlet will be less loaded.

Proof for Theorem 1 The proof is presented by using mathematical induction.

- for an odd number of nodes in the ring

Firstly, we note that adding two nodes to the ring (independently of the original number of nodes in the ring— n) will increase N_x by $\frac{N-1}{2}$, where N is the number of nodes in the ring with two nodes added ($N = n + 2$). This situation takes

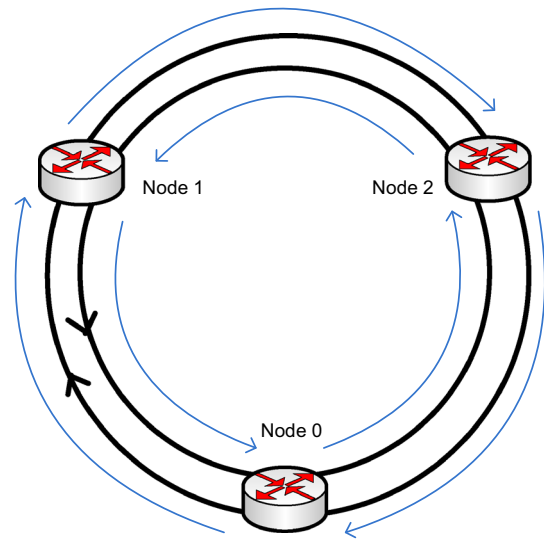


Fig. 7 Traffic flows in RPR ring with 3 nodes when all nodes send traffic to each other

place because each node in the bigger ring will have to send traffic flows to the new nodes and the new nodes will have to send traffic to the other nodes in the ring. As a result, $\frac{N-1}{2}$ new flows will be transmitted through the outer ring, and the same number of flows will be sent through the inner ring.

For $n = 3$ we have:

$$N_x = \frac{n^2 - 1}{8} = 1 \quad (3)$$

and this is correct as we can see in Fig. 7.

For $N = n + 2$ we have:

$$N_{x+2} = \frac{(n + 2)^2 - 1}{8} = \frac{n^2 + 4n + 4 - 1}{8} = N_x + \frac{4n + 4}{8} = N_x + \frac{n + 1}{2} = N_x + \frac{N - 1}{2} \quad (4)$$

which finishes this part of the proof.

- for an even number of nodes in the ring

Firstly, we note that adding two nodes to the ring (independently of the original number of nodes in the ring— n) will increase the N_x index by $\frac{N}{2}$ for the outer ring and by $\frac{N}{2} - 1$ for the inner ring, where N is the number of nodes in the ring with two nodes added ($N = n + 2$). As a result, $\frac{N}{2}$ new flows will be transmitted through the outer ring, and $\frac{N}{2} - 1$ new flows will be sent through the inner ring.

For $n = 4$ we have:

for the outer ring:

$$N_x = \frac{n^2}{8} + \frac{n}{4} = 3 \quad (5)$$

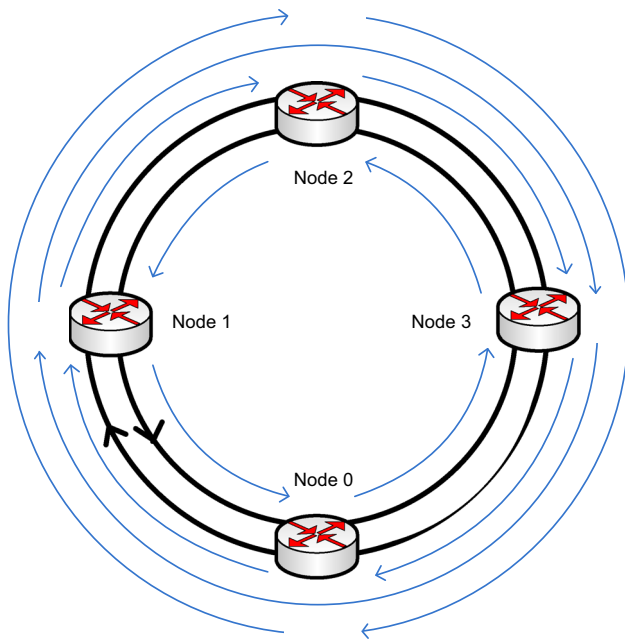


Fig. 8 Traffic flows in RPR ring with 4 nodes when all nodes send traffic to each other

for the inner ring:

$$N_x = \frac{n^2}{8} - \frac{n}{4} = 1 \tag{6}$$

and this is correct as we can see in Fig. 8.

For $N = n + 2$

for the outer ring:

$$\begin{aligned} N_{x+2} &= \frac{(n+2)^2}{8} + \frac{n+2}{4} = \frac{n^2 + 4n + 4}{8} + \frac{n}{4} + \frac{1}{2} \\ &= N_x + \frac{n+2}{2} = N_x + \frac{N}{2} \end{aligned} \tag{7}$$

for the inner ring:

$$\begin{aligned} N_{x+2} &= \frac{(n+2)^2}{8} - \frac{n+2}{4} = \frac{n^2 + 4n + 4}{8} - \frac{n}{4} - \frac{1}{2} \\ &= N_x + \frac{n+1}{2} - \frac{1}{2} = N_x + \frac{N}{2} - 1 \end{aligned} \tag{8}$$

which finishes the proof. □

5.2 Multi-ring topologies

When considering multi-ring topologies, we have to divide the ring into a finite number of rings. The analysis presented below is provided for a FARR network composed of two rings.

- the ring with an odd number of nodes may be divided into one ring with an odd number of nodes (a) and one with an even number of nodes (b), where $a + b = n$ and n is the number of nodes in the original ring

for the first ring (with an odd number of nodes):

$$N_x = \frac{a^2 - 1}{8} + \frac{a - 1}{2}(n - a) \quad \text{for both ringlets} \tag{9}$$

for the second ring (with an even number of nodes):

$$N_x = \begin{cases} \frac{b^2}{8} - \frac{b}{4} + (\frac{b}{2} - 1)(n - b) & \text{for inner ringlet} \\ \frac{b^2}{8} + \frac{b}{4} + \frac{b}{2}(n - b) & \text{for outer ringlet} \end{cases} \tag{10}$$

- the ring with an even number of nodes may be divided into one ring with an odd number of nodes (a) and a second also with an odd number of nodes (b), where $a + b = n$ and n is the number of nodes in original ring

for the first ring with an odd number of nodes:

$$N_x = \frac{a^2 - 1}{8} + \frac{a - 1}{2}(n - a) \quad \text{for both ringlets} \tag{11}$$

for the second ring with an odd number of nodes:

$$N_x = \frac{b^2 - 1}{8} + \frac{b - 1}{2}(n - b) \quad \text{for both ringlets} \tag{12}$$

- the ring with an odd number of nodes may be divided into one ring with an even number of nodes (a) and a second with an even number of nodes (b), where $a + b = n$ and n is the number of nodes in the original ring

for the first ring with an even number of nodes:

$$N_x = \begin{cases} \frac{a^2}{8} - \frac{a}{4} + (\frac{a}{2} - 1)(n - a) & \text{for inner ringlet} \\ \frac{a^2}{8} + \frac{a}{4} + \frac{a}{2}(n - a) & \text{for outer ringlet} \end{cases} \tag{13}$$

for the second ring with an even number of nodes:

$$N_x = \begin{cases} \frac{b^2}{8} - \frac{b}{4} + (\frac{b}{2} - 1)(n - b) & \text{for inner ringlet} \\ \frac{b^2}{8} + \frac{b}{4} + \frac{b}{2}(n - b) & \text{for outer ringlet} \end{cases} \tag{14}$$

The presented equations may be easily extended for any multi-ring topology.

In Table 4, the values of N_x for several configurations of FARR networks are presented. The results are calculated

Table 4 Maximum number of flows sharing one link (N_x) in two FARR topologies

No. of nodes		Single-ring topology		Two-ring topology			
One ring	Two rings	Inner ring	Outer ring	1st ring		2nd ring	
n nodes	a/b nodes	(N_x)	(N_x)	Inner ring (N_x)	Outer ring (N_x)	Inner ring (N_x)	Outer ring (N_x)
6	3/3	3	6	<u>4</u>	<u>4</u>	<u>4</u>	<u>4</u>
8	4/4	<u>6</u>	<u>10</u>	5	11	5	11
9	5/4	<u>10</u>	<u>10</u>	11	11	6	13
10	5/5	10	15	<u>13</u>	<u>13</u>	<u>13</u>	<u>13</u>
11	5/6	<u>15</u>	<u>15</u>	15	15	13	21
14	7/7	21	28	<u>27</u>	<u>27</u>	<u>27</u>	<u>27</u>

for a single-ring topology composed of n nodes, and for each ring in a two-ring topology composed of a and b nodes where $a + b = n$. The results for the better topology for each case are underlined. We can see that it is profitable to divide a ring with an even number of nodes into two rings with an even number of nodes. For example, in one ring composed of six nodes, each flow in the outer ring receives 1/6 of link capacity, while in two rings composed of three nodes and connected by a bridge, each flow may consume 1/4 of total capacity. The equations and analysis presented in this section may help network administrators to make a decision about topology reconfiguration when the number of nodes in their FARR network changes. For example, they may calculate that traffic will be sent faster if they divide one big FARR ring into several smaller rings connected by bridges or inter-nodes. Based on the statistics in their network, they may discover which links are highly loaded and which are used rarely. Based on this knowledge, they may divide a ring into two or more connected rings in such a way that the volume of traffic sent between rings is minimized and the overall bandwidth is better utilized.

6 Conclusion

The concept of a new architecture—a FARR for LAN and MAN networks is proposed and analyzed. FARR networks combine the advantages of Resilient Packet Ring and FAN. In the solution presented, traffic is served as flows and implicitly classified into one of two traffic types: streaming or elastic. Streaming flows are served with high priority over elastic ones. The bandwidth not used by streaming flows is fairly divided among elastic flows. FARR networks ensure good scalability and effective protection mechanisms (steering or wrapping) which ensure fast redirection of the streaming traffic in case of failure. Moreover, FARR conforms to the net neutrality paradigm.

The RPAEF congestion control mechanism along with the limiting mechanism ensure fast acceptance of streaming

flows without deteriorating network performance. Moreover, the implementation of the GPFL in each router in the ring ensures continuous transmission (without outages) of streaming flows even when a network element fails.

The fairness and automatic reconfiguration mechanisms proposed for use in FARR rings seem to be efficient and widely accepted features applicable when designing novel metro networks. The analysis, which is the main contribution of the paper, shows the usefulness of implementing multi-ring topologies. As many operators are facing the necessity of reorganizing metro networks, FARR can be considered the solution of choice, showing its flexibility and improved performance. The availability of an intelligent optical layer, such as ASON or GMPLS, makes the proposal of adaptively reconfigured multi-ring FARR networks an interesting solution for next generation metros.

Open Access This article is distributed under the terms of the Creative Commons Attribution 4.0 International License (<http://creativecommons.org/licenses/by/4.0/>), which permits unrestricted use, distribution, and reproduction in any medium, provided you give appropriate credit to the original author(s) and the source, provide a link to the Creative Commons license, and indicate if changes were made.

References

1. Cochrane, P. (2006). Net neutrality or suicide? *Proceedings of the IEEE*, 94, 1779–1780.
2. Bianciotto, A., Gaudino, R. (2004). WONDER: Overview of a packet-switched MAN architecture. In *Proceedings of the OpNeTec*, Pisa, Italy.
3. Nord, M., Bjornstad, S., & Nielsen, M. (2005). Distributed MAC protocol for optical packet switched ring network supporting variable length packets. *OSA Journal on Optical Networking*, 4, 213–225.
4. Finochietto, J. M., Neri, F., Wajda, K., Watzka, R., Domzał, J., & Zouganeli, M. N. E. (2008). Towards optical packet switched MANs: Design issues and tradeoffs. *Optical Switching and Networking (OSN)*, 5, 253–267.
5. Cosares, S., & Saniee, I. (1994). An optimization problem related to balancing loads on SONET rings. *Telecommunication Systems*, 3, 165–181.

6. Domzal, J., Wajda, K., Jajszczyk, A. (2010). Flow-aware resilient ring. In *IEEE ICC 2010*, Cape Town, South Africa.
7. 802.17 IEEE Standard, 2004.
8. Cinkler, T. (2011). Some more aspects of resilience. *Telecommunication Systems*, 52(2), 825–846.
9. Roberts, J., & Oueslati, S. S. (2000). Quality of service by flow aware networking. *Philosophical Transactions of The Royal Society of London*, 358, 2197–2207.
10. Kortebe, A., Oueslati, S., Roberts, J. (2004). Cross-protect: Implicit service differentiation and admission control. In *IEEE HPSR 2004*, Phoenix, USA.
11. Karol, M., Krishnan, P., & Li, J. J. (2005). VoIP protection and performance improvement. *Telecommunication Systems*, 28, 351–367.
12. Dynamic packet transport technology and performance. Cisco System White Paper (2000).
13. Tsiang, D., Suwala, G. (2000). The Cisco SRP MAC Layer Protocol, RFC 2892.
14. Blake, S., Black, D., Carlson, M., Davies, E., Wang, Z., Weiss, W. (1998). *An architecture for differentiated services* IETF RFC 2475.
15. Braden, R., Clark, D., Shenker, S. (1994). *Integrated services in the internet architecture an overview* IETF RFC 1633.
16. Wang, S., Xuan, D., Bettati, R., & Zhao, W. (2010). Toward statistical QoS guarantees in a differentiated services network. *Telecommunication Systems*, 43, 253–263.
17. ITU-T, Network grade of service parameters and target values for circuit-switched services in the evolving ISDN, Recommendation ITU-T E.721 (1999).
18. Kortebe, A., Oueslati, S., Roberts, J. (2005). Implicit service differentiation using deficit round robin. In *ITC19*, Beijing, China.
19. Domzal, J., Jajszczyk, A. (2009). Approximate flow-aware networking. In *IEEE ICC 2009* Dresden, Germany.
20. Kortebe, A., Muscariello, L., Oueslati, S., Roberts, J. (2004). On the scalability of fair queueing. In *ACM HotNets-III* San Diego, USA.
21. Joung, J., Song, J., & Lee, S. S. (2008). Flow-based QoS management architectures for the next generation network. *ETRI Journal*, 30, 238–248.
22. Jain, R. (2011). Architectures for the next generation internet and the future networks. In *IEEE ICC 2011—tutorial* Kyoto, Japan.
23. Cholda, P., Domzal, J., Jajszczyk, A., Wajda, K. (2006). Reliability analysis of resilient packet rings. In *Safecomp'06* Gdansk, Poland.
24. Domzal, J., Wojcik, R., Jajszczyk, A. (2008). The impact of congestion control mechanisms on network performance after failure in flow-aware networks. In *Proceedings of international workshop on traffic management and traffic engineering for the future internet, FITraMEn 2008* Porto, Portugal.
25. Domzal, J., Wojcik, R., Wajda, K., Jajszczyk, A., Lopez, V., Hernandez, J. A., Aracil, J., Cardenas, C., Gagnaire, M. (2009). A multi-layer recovery strategy in fan over wdm architectures. In *DRCN 2009*, Washington DC, USA.
26. Domzal, J., Wojcik, R., Jajszczyk, A. (2009). Reliable transmission in flow-aware networks. In *IEEE Globecom 2009* Honolulu, USA.
27. Lopez, V., Cardenas, C., Hernandez, J.A., Aracil, J., Gagnaire, M. (2008). Extension of the flow-aware networking (FAN) architecture to the IP over WDM environment. In *4th international telecommunication networking workshop on QoS in multiservice IP networks, 2008. IT-NEWS 2008* (pp. 101–106) Venice.
28. Domzal, J., & Jajszczyk, A. (2008). New congestion control mechanisms for Flow-Aware Networks. In *IEEE ICC 2008* Beijing, China.
29. SAS—spatially aware bridging over RPR, 802.17b IEEE Standard (2007).



Jerzy Domzał received the M.S. and Ph.D. degrees in Telecommunications from AGH University of Science and Technology, Krakow, Poland in 2003 and 2009, respectively. Now, he is an Assistant Professor at Department of Telecommunications at AGH University of Science and Technology. He is especially interested in optical networks and services for future Internet. He is an author or co-author of many technical papers, four patent applications and one book. International trainings: Spain, Barcelona, Universitat Politècnica de Catalunya, April 2005; Spain, Madrid, Universidad Autónoma de Madrid, March 2009, Stanford University, USA, May-June 2012.