Flow-Aware Resilient Ring

Jerzy Domżał[1], Krzysztof Wajda[1], Andrzej Jajszczyk[2]
[1]*Member, IEEE*, [2]*Fellow, IEEE*

***Abstract*—A new proposal for Metropolitan Area Networks is presented and analyzed in the paper. The Flow-Aware Resilient Ring (FARR) combines the best features of two known network architectures: Flow-Aware Networking and Resilient Packet Ring. Transmitted traffic in FARR networks is based on implicitly classified flows which allows for providing Quality of Service guaranties in accordance with network neutrality rules. Moreover, the traffic with high priority is protected by the steering mechanism which ensures fast traffic redirection in time less than 50 ms. The advantages and weaknesses of the proposed architecture and new solutions to be used in it are described and analyzed in the paper. Moreover, it is shown that simultaneous implementation of all of them ensures fast, scalable and reliable transmission of streaming flows in FARR.**

***Index Terms*—Flow-Aware Networks; Resilient Packet Ring; Quality of Service; congestion control; reliability**

I. Introduction

The modern Metropolitan Area Networks (MANs) have to be fast, resilient and consistent with the net neutrality concept [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 the European Union projects, like WONDER, SWRON, or OPSRN [2], [3]. Each of them has advantages and disadvantages. For example, SONET/SDH networks were designed for carrier-class performance and reliability, and for circuit-switched operation. It causes that 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 are usually at a very initial stage and a lot of research and implementation effort is needed.

In this paper, we propose a new solution called Flow-Aware Resilient Ring (FARR), which 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 [4]. It is a technology which supports data transfer in a dual counter-rotating ring topology. Generally, RPR was designed as an universal technology which can be used in local, metropolitan and wide area networks. Restoration mechanisms of RPR ensure automatic reaction to failures in time less than 50 ms. FAN was proposed in [5] by J. Roberts and S. Oueslati. The complete architecture was presented in 2004 in [6]. In FAN, traffic is served as flows and implicitly classified to one of two types: elastic or streaming. It allows for providing QoS guaranties with respect to the net neutrality paradigms.

This paper is organized as follows. Section II describes the RPR and FAN concepts. Section III shows the assumptions and the description of the new FARR proposal. In Section IV, the congestion control mechanism RPAEF and the mechanism for limiting the number of new flows accepted in the FAN routers are presented. The concept of the GPFL (*Global Protected Flow List*) in FARR networks is analyzed in Section V. The results of carefully selected simulation experiments for each new solution are presented at the ends of the related sections. Section VI concludes the paper.

II. RPR and FAN basics

A. Resilient Packet Ring

RPR is based on DPT (*Dynamic Packet Transport*), proprietary protocol proposed by Cisco [7] and inherits many its features, including:

- enhanced protection,
- interoperability with major transmission standards,
- scalability in speeds and number of nodes,
- 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 composed of up to 255 nodes and of the maximum circumference lower than 2000 km. Packets are transmitted in both rings simultaneously in opposite directions. When data packets are transmitted in outer ring, control packets corresponding to them are transmitted in the second one. The protocol is designed to operate over a variety of physical layers. RPR is equipped with OAM features, advanced traffic management features and bandwidth management (leaky bucket) component.

One of the main advantages of RPR is fast reaction to 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 by failed links or nodes;
- *wrapping protection* — activated only in nodes which declared it during the topology discovery process; after failure packets are redirected in a node located next to the failed link or node and sent in the other ring.

The topology discovery mechanism is used to allow fast reaction to topology change. It is activated when an RPR

J. Domżał, K. Wajda and A. Jajszczyk are with the Department of Telecommunications, AGH University of Science and Technology, Al. Mickiewicza 30, 30-059 Kraków, Poland (e-mail: {domzal, wajda, jajszczyk}@kt.agh.edu.pl).

978-1-4244-6404-3/10/$26.00 ©2010 IEEE

network is set and each time when a node or link fails or topology changes (e.g., when a node id added to the ring or removed). Moreover, topology discovery packets are also sent periodically to ensure proper topology map distribution. Data transmission in RPR networks is possible if each node receives topology discovery packets and, based on them, builds the topology map.

RPR supports three traffic classes: low, medium and high priority (C, B and A respectively). The high priority traffic has an absolute priority over the low priority traffic. The low priority traffic is shaped in the RPR nodes to achieve fairness among competing traffic streams. For medium priority traffic a contract is needed. The "in-contract" part of medium priority traffic is treated as high priority traffic, while the out-of-contract part of traffic is sent as low priority traffic or dropped.

The fairness algorithm is implemented to ensure efficient bandwidth allocation. It is used for low and medium priority traffic (class B and C respectively). All available bandwidth is fairly shared between nodes sending data. Moreover, thanks to the fact that data packets are destination stripped, it is possible to transmit more data (in comparison to e.g., FDDI networks) at the same time in different parts of rings. There are two fairness algorithm versions in RPR:

- *conservative mode* — message with new fair rate value is sent if all stations in the congestion domain adjusted to the fair rate;
- *aggressive mode* — messages with new fair rate value are sent periodically with a default interval of 100 s.

B. Flow-Aware Networks

The main goal of FAN is to ensure the proper quality of service (QoS) in packet networks in an implicit way and by using only the minimal knowledge of the network. These features cause that FAN differs from well known QoS architectures, like DiffServ (*Differentiated Services*) [8] or IntServ (*Integrated Services*) [9]. In particular, FAN is easier to implement and conforms to the net neutrality paradigms.

The basic assumption of FAN is that traffic is sent as flows and served in the cross-protect routers (also denoted as XP's) [6]. There are two traffic types defined in 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 implicitly classified to one of the presented types based on the queues occupation and, then, served with (streaming) or without (elastic) priority.

The main elements of the cross-protect routers are: the admission control block (AC), which decides of accepting or rejecting packets of flows and the scheduler, which is responsible for packet queuing and periodical 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 PFL (*Protected Flow List*). 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.

A new flow may begin transmission only if its identifier is accepted in the admission control block and written to the PFL. A FAN link may be in one of two states: congestion or congestion-less. In the first case, only the packets of flows which IDs are written to the PFL may be served while other packets are discarded. It means that sometimes a new flow has to wait for a long time before it is allowed to begin transmission. This situation is unacceptable for the real-time applications, like e.g., VoIP (*Voice over IP*) or VoD (*Video on Demand*). The congestion case 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*). We have to note that in almost every case the congestion is indicated by the *fair_rate* parameter. In the congestion-less state each new flow is accepted and begins transmission immediately.

Two scheduling algorithms were proposed to be used in FAN, PFQ (*Priority Fair Queuing*) or PDRR (*Priority Deficit Round Robin*). Because of lack of space we omit the description of them. It can, however, be found in [6] and [10]. There is also a new proposal, called AFAN (*Approximate Flow-Aware Networking*), which assumes usage of the AFD (*Approximate Fair Dropping*) algorithm for scheduling packets [11]. 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 and AFAN are similar to those obtained for FAN with the PFQ.

FAN is a scalable solution. The complexity of queuing algorithms does not increase with the link capacity [12] because the number of active flows is almost stable. It is important to note that 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 signaling and very low data handling complexity, the scalability of FAN is achieved and not matched by any other architecture [13].

The flow identification process is based on five parameters: the transport protocol, source and destination addresses, and port numbers. No other packet labels are needed and expected. Moreover, the flow differentiation is based only on the internal, implicit node decisions. This way, services in a network may be differentiated, while the fairness and neutrality are maintained.

III. Flow-Aware Resilient Ring

RPR is a well known standard implemented in many countries, e.g., USA or China. While it is a stable solution it still needs improvements. 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 solution is to use the DS field in the header of IP packet. In IPv4 it is the ToS (*Type of Service*) byte while in the IPv6 it is the TC (*Traffic Class*) byte. Such a concept has a few known drawbacks. For example, it does not assume that malicious users may try to change the values of the DS field to speed up their transmission. Moreover, the method of such 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 a traffic generated by other network users. In the most rigourous 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 of net neutrality, traffic should be served without explicit classification but may be sent in different ways based on implicit classification (without ISPs interference). It means that the values written to the DS field will have to be ignored by routers connected to the source nodes. One of the most important advantages of RPR is its reliability [14]. Protection and topology discovery mechanisms ensure fast traffic redirection in time less than 50 ms.

The problems presented for RPR networks are not observed in Flow-Aware Networks. In FAN, traffic is implicitly classified and it is not possible to force a special treatment of traffic from cross-protect routers. The high priority traffic is identified based only on traffic characteristics and served as first in the routers. It ensures conformity with the net neutrality paradigm. While FAN works well under normal conditions, there are still some problems which have to be solved when considering a reliable transmission. In a case of a network element failure, traffic usually needs to be redirected to the other route. As shown in [15], if traffic is redirected to the congested link not all streaming flows are accepted again in a short time, which is very unfavorable for users making e.g., phone calls or participating in a video conference. On the other hand, if traffic is redirected to the 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 [16], the 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 if only there are enough resources. If it is impossible the traffic needs to be redirected in the IP layer. Paper [17] presents the concept of GPFL (*Global Protected Flow List*), which in some cases ensures fast redirection. The authors of [18] suggest that excessive traffic, which cannot be accepted in XP routers may be sent directly using the optical domain. In each of these solutions, a significant effort is needed to ensure correct and fast reaction to a failure.

Flow-Aware Resilient Ring (FARR) presented in this paper combines advantages of both architectures described above. In FARR we assume the ring topology. The neighbor nodes are connected by two single one-way links (in opposite directions). The routers are cross-protected. As packets are destination stripped, the spatial reuse is allowed. The traffic is sent as flows (elastic or streaming) without any packet marking and signaling. Only the topology discovery protocol is implemented to ensure proper behavior of protection mechanisms (steering or wrapping). The streaming flows are sent with priority and the 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. 1. The topology presented in this figure was our reference topology in simulation experiments.

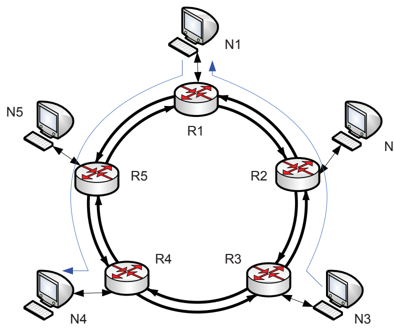

Fig. 1. Reference topology of FARR network

A. Simulation analysis of FARR network

In this and following sections we present the results of carefully selected simulation experiments carried out in the ns-2 simulator. Basic simulation parameters are presented in each section. The detailed description of the simulation environment is given in [19].

The simulation analysis, presented in this section, was provided to show how the FARR networks work. In the first experiment we decided to check how long the streaming flows have to wait for acceptance in a congested FARR network.

We made 50 simulation runs in various conditions. The duration of each simulation run was set to 500 s to observe acceptance times of 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. The elastic flows were sent as follows: from N1 to N4, from N2 to N5, from N3 to N1, from N4 to N2, from N5 to N3. Such an assignment caused 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. We decided to provide the traffic pattern with Pareto distribution for calculating the volume of traffic to be sent by the elastic flows (ftp connections). The exponential distribution for generating the time intervals between beginnings of the transmissions of the elastic flows as well as for generating the start times of streaming flows was used. 20 streaming flows were sent by node N3 to N1 and other 20 streaming flows were sent from node N1 to N4 (see Fig. 1). In both cases traffic was sent through the outer link based on the information from the topology discovery protocol. We decided to analyze the VoIP connections realizing the Skype service. 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 the background traffic and used to saturate the analyzed links. It was assumed that the capacity of links between routers was set to 100 Mbit/s and the PFQ algorithm was implemented. The capacity of access links (with FIFO queues) was set to 1 Gbit/s. The buffers in XP routers were sized to 1000 packets which is a reasonable value for FAN 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 of *waiting_time* (acceptance time of streaming flows) in each router on their routes are presented in Tab. I.

TABLE I
THE *waiting_time* VALUES OF STREAMING FLOWS IN ROUTERS

No.	R5	R4	R3	R2
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

The results show that streaming flows are accepted after tens of seconds in the first routers on their routes and after about a hundred of seconds in the seconds routers. It 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 [20], the setup time (post-selection delay) of local calls should be less than 6 s while for the international calls it should not exceed 11 s. The second conclusion is that acceptance times of streaming flows does not depend on the number of elastic flows active in background. Therefore, for simplicity, in the following experiments, we assumed the constant value (200) of elastic flows sent by each node.

IV. The RPAEF and limiting mechanisms

In this section, we present the RPAEF (*Remove and Prioritize in access Active Elastic Flows*) congestion control mechanism, which allows for decreasing the acceptance times of streaming flows in XP routers. The mechanism was firstly presented in [17]. The principle operation of the RPAEF mechanism is presented in the following paragraph.

If a packet of a new flow arrives at the AC block of an XP router in congestion it is checked if the PAFL (*Priority in Access Flow List*) is empty. If so, the packet is discarded and the IDs of elastic flows being active for at least $active\_time$ are removed from the PFL and written to the PAFL for a short time. On the other hand, if the PAFL is not empty when a packet of a new flow arrives it may be accepted in two ways. If ID of the corresponding flow is in the PAFL the packet is accepted. On the other side, if this flow ID is not in the PAFL the incoming packet is accepted with small probability P_{RPAEF} (e.g., 0.03). Of course, in the congestion-less state packets of each flow are accepted.

The idea of this solution is to ensure a quick acceptance time of new streaming flows without breaks in transmission of elastic flows which identifiers are 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}. In such a case the UDP flows with small packets (streaming flows) have much more chances for acceptance than the TCP flows with bigger packets. That is why the streaming flows has the precedence in acceptance over elastic ones.

While the RPAEF mechanism ensures good performance for streaming flows there is a need to decrease the number of elastic flows accepted in the routers. If the number of elastic active flows is too large it is not possible to serve them with guaranteed minimum acceptable fair rate. To deal with this problem the 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:

$$\begin{cases} N = 100/(min\_fair\_rate \times i) & \text{if } i > 0 \\ N = \infty & \text{if } i = 0 \end{cases} \tag{1}$$

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*. Such value of i was assumed in our following simulation experiments based on results presented in [17].

A. Simulation analysis of FARR with RPAEF and limiting mechanisms

The simulation experiment is illustrated by Fig. 2. We made 20 simulation experiments (10 with steering and 10 with wrapping). The simulation parameters were exactly the same as in the previous experiment. We only assumed that each node sends constant number of elastic flows (200) and at 200 s the links between routers R1 and R2 fail. Moreover, we decided that node N3 sends 200 elastic flows to node N5. It ensured that inner links between routers R3 and R5 were congested. Two cases were considered: the failure was repaired by the steering (Fig. 2a) or wrapping (Fig. 2b) mechanism. We can see that the wrapping mechanism lengthens the route after failure in comparison to the steering one. It increases the acceptance time of redirected flows. We assumed that the steering mechanism is better and the results of simulation experiments are presented for network presented in Fig. 2a.

The analysis was provided 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. 3 show the acceptance times of 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 increase also with increasing values of the *active_time* parameter, that is, when the IDs of elastic flows are removed from the PFL less frequently. We have to note, that according to [20], the 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. 4 show the mean number of elastic flows accepted in router R2 (before failure). We can 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 the 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 which should be used in the RPAEF mechanism.

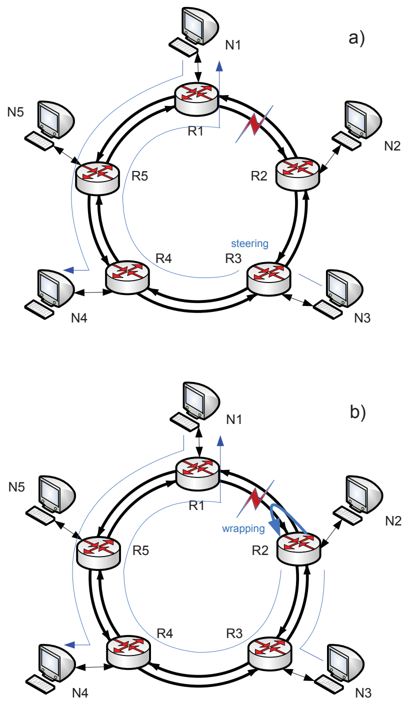

Fig. 2. FARR network: a) failure repaired by steering mechanism, b) failure repaired by wrapping mechanism

The results presented in Tab. II show the mean acceptance times of 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 transmission of streaming flows 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 we present a new mechanism which meets this requirement.

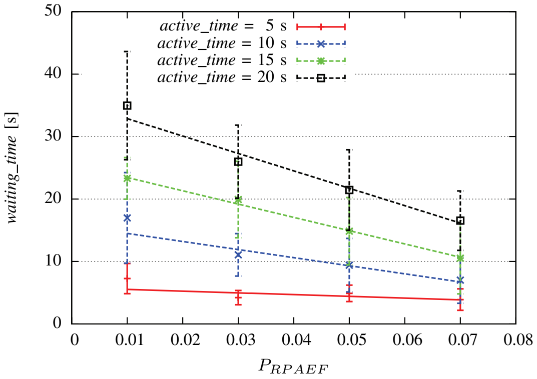

Fig. 3. Acceptance times of streaming flows in FARR with RPAEF

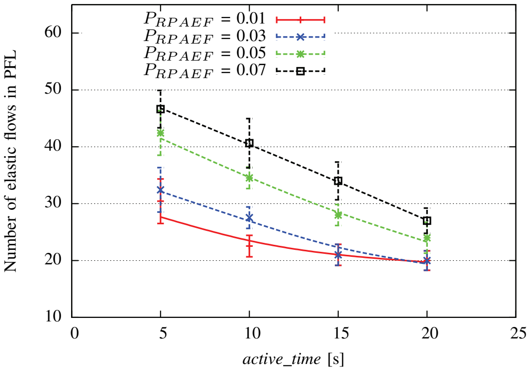

Fig. 4. Number of elastic flows accepted in the PFL in FARR with RPAEF

V. Global Protected Flow List in FARR

To improve the network performance after failure in FARR networks we propose to use the concept of GPFL (*Global Protected Flow List*). The pseudocode for realizing the functionality of the GPFL in FARR networks is presented in Tab. III. We implemented the global list 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 an information if a flow is streaming or elastic. This condition is checked each time when 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 the 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 the congestion state it is accepted if its ID is in the GPFL and it is a streaming flow. It allows for immediate acceptance of redirected streaming flows in a router realizing the steering protection.

TABLE II
THE *waiting_time* VALUES ON A BACKUP ROUTE OF STREAMING FLOWS

waiting_time/i	**R3**	**R4**	**R5**
-/-	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

We use the DS field mentioned before in Sec. III to mark the first packets of redirected streaming flows. We assumed to set DS=0 in the header of each packet incoming from a source node (line 2). If a router see 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 criterium) (lines 10-11).

A. Simulation analysis of FARR with RPAEF, limiting mechanisms and GPFL

We made 10 simulation runs in the same conditions as in the previous experiment but with the implemented GPFL. The simulation results show that the redirected streaming flows (under the control of the steering mechanism) were accepted immediately in each router on their new route and the performance of the network was achieved on the invariable level.

TABLE III
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
```

VI. CONCLUSION

The concept of a new architecture Flow-Aware Resilient Ring proposed for LAN and MAN networks is proposed and analyzed in the paper. FARR networks combine the advantages of Resilient Packet Ring and Flow-Aware Networks. In our solution, traffic is served as flows and implicitly classified to one of two traffic types: streaming or elastic. The streaming flows are served with a high priority over elastic ones. The bandwidth not used by streaming flows is fairly divided among elastic flows. FARR networks ensure a good scalability and very good protection mechanisms which ensure fast redirection of the streaming traffic. Moreover, they conform to the net neutrality paradigm.

The RPAEF congestion control mechanism along with the limiting mechanism ensure fast acceptance of streaming flows without deteriorating a network performance. Moreover, the implementation of the GPFL in each router in the ring ensures continuous transmission (without outages) of streaming flows even in a case when a network element fails.

The new proposal of the network architecture presented in the paper meets the requirements of modern networks and may be used in the future Internet.

REFERENCES

[1] P. Cochrane, “Net Neutrality or Suicide?” *Proceedings of the IEEE*, vol. 94, pp. 1779–1780, Oct. 2006.

[2] A. Bianciotto and R. Gaudino, “WONDER: overview of a packet-switched MAN architecture,” in *Proceedings of the OpNeTec*, Pisa, Italy, Oct. 2004.

[3] J. M. Finochietto, F. Neri, K. Wajda, R. Watza, J. Domzal, and M. N. E. Zouganeli, “Towards Optical Packet Switched MANs: Design Issues and Tradeoffs,” *Optical Switching and Networking (OSN)*, vol. 5, pp. 253–267, Oct. 2008.

[4] *802.17 IEEE Standard*, June 2004.

[5] J. Roberts and S. S. Oueslati, “Quality of Service by Flow Aware Networking,” *Philosophical Transactions of The Royal Society of London*, vol. 358, pp. 2197–2207, Sept. 2000.

[6] A. Kortebi, S. Oueslati, and J. Roberts, “Cross-protect: implicit service differentiation and admission control,” in *IEEE HPSR 2004*, Phoenix, USA, Apr. 2004.

[7] D. Tsiang and G. Suwala, “The Cisco SRP MAC Layer Protocol,” RFC 2892, Aug. 2000.

[8] S. Blake, D. Black, M. Carlson, E. Davies, Z. Wang, and W. Weiss, “An Architecture for Differentiated Services,” IETF RFC 2475, Dec. 1998.

[9] R. Braden, D. Clark, and S. Shenker, “Integrated Services in the Internet Architecture an Overview,” IETF RFC 1633, June 1994.

[10] A. Kortebi, S. Oueslati, and J. Roberts, “Implicit Service Differentiation using Deficit Round Robin,” in *ITC19*, Beijing, China, Aug.-Sept. 2005.

[11] J. Domzal and A. Jajszczyk, “Approximate Flow-Aware Networking,” in *IEEE ICC 2009*, Dresden, Germany, June 2009.

[12] A. Kortebi, L. Muscariello, S. Oueslati, and J. Roberts, “On the scalability of fair queueing,” in *ACM HotNets-III*, San Diego, USA, Nov. 2004.

[13] J. Joung, J. Song, and S. S. Lee, “Flow-Based QoS Management Architectures for the Next Generation Network,” *ETRI Journal*, vol. 30, pp. 238–248, Apr. 2008.

[14] P. Cholda, J. Domzal, A. Jajszczyk, and K. Wajda, “Reliability Analysis of Resilient Packet Rings,” in *Safecomp’06*, Gdansk, Poland, Sept. 2006.

[15] J. Domzal, R. Wojcik, and A. Jajszczyk, “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, Dec. 2008.

[16] J. Domzal, R. Wojcik, K. Wajda, A. Jajszczyk, V. Lopez, J. A. Hernandez, J. Aracil, C. Cardenas, and M. Gagnaire, “A Multi-layer Recovery Strategy in FAN over WDM Architectures,” in *DRCN 2009*, Washington DC, USA, Oct. 2009 (to be published, available at: http://www.kt.agh.edu.pl/∼jdomzal/drcn09.pdf).

[17] J. Domzal, R. Wojcik, and A. Jajszczyk, “Reliable Transmission in Flow-Aware Networks,” in *IEEE Globecom 2009*, Honolulu, USA, Nov.-Dec. 2009 (to be published, available at: http://www.kt.agh.edu.pl/∼jdomzal/globecom09.pdf).

[18] V. Lopez, C. Cardenas, J. A. Hernandez, J. Aracil, and M. Gagnaire, “Extension of the flow-aware networking (FAN) architecture to the IP over WDM environment,” in *Telecommunication Networking Workshop on QoS in Multiservice IP Networks, 2008. IT-NEWS 2008. 4th International*, Venice,, Feb. 2008, pp. 101–106.

[19] http://www.kt.agh.edu.pl/∼jdomzal/sim_param_icc2010.pdf.

[20] ITU-T, “Network grade of service parameters and target values for circuit-switched services in the evolving ISDN,” Recommendation ITU-T E.721, May 1999.

2010 IEEE International Conference on Communications

Communications: Accelerating Growth and Development

IEEE
INTERNATIONAL CONFERENCE
ON COMMUNICATIONS
ICC 2010

CapeTown, South Africa
23 - 27 May

Welcome

Getting Started

Conference Information

Days

Symposia

Authors

Search

IEEE

IEEE
COMMUNICATIONS
SOCIETY

Conference Information

Copyright

2010 IEEE International Conference on Communications

Copyright and Reprint Permissions

IEEE Catalog Number: CFP10ICC-CDR
ISBN: 978-1-4244-6403-6

Printed copies of this publication are available from:

Curran Associates, Inc
57 Morehouse Lane
Red Hook, NY 12571 USA
Phone: (845) 758-0400
Fax: (845) 758-2633
E-mail: curran@proceedings.com

Produced by IEEE eXpress Conference Publishing
For information about producing a conference proceedings and receiving an estimate, contact
conferencepublishing@ieee.org
http://www.ieee.org/conferencepublishing

Main Menu