Overview of the Evolving IEEE 802.17 Resilient Packet Rings Standard

Khaled M. F. Elsayed
(khaled@ieee.org)

Department of Electronics and Communications Engineering
Faculty of Engineering, Cairo University, Giza, Egypt 12613

Keywords: Resilient Packet Rings, Media Access Control, Bandwidth Management, Fairness, Protection Switching.

Abstract: We present an overview of the IEEE 802.17 Resilient Packet Ring (RPR) protocol standard for metropolitan area networks. We discuss the main characteristics of the protocol and the main drivers for its development. We outline various aspects of the protocol: architecture and operation principles, physical layer, packet formats, the MAC protocol and its fairness, protection switching and topology discovery. We also discuss possible ways and technologies that could be used by a carrier to evolve its services and network architecture to meet the ever-increasing demand for bandwidth in the metropolitan area.

1. INTRODUCTION

The IEEE 802.17 Resilient Packet Ring (RPR) protocol [2] is one of the newest members of the 802.x family of protocols. The protocol is being targeted for deployment in metropolitan-area networks (MANs) based on optical-fiber rings. The explosion in end-user demand for versatile high-speed (and low cost) connectivity in the metropolitan area is the main driver for introducing this new protocol. Applications such as large data centers, web hosting farms, corporate LAN interconnection, campus networking, and ISP interconnection to backbone networks, are examples of services needing such connectivity.

Earlier MAN protocols such as DQDB [3] are limited in bandwidth and have not been deployed with much success in carrier networks. SDH/SONET ring architecture has existed for a long time in the service provider environment. SDH/SONET rings offer access rates from STM-1/OC-3 to STM-64/OC-192 speeds and implement attractive capabilities such as self-healing via automatic protection switching and proactive performance monitoring. On the other hand, SDH/SONET based metro networks are based on time-division multiplexing and therefore are not efficient for the bursty (and self-similar) LAN traffic [13]. So, whether the user has traffic or not, capacity on the ring is reserved at any time. The RPR protocol tries to solve the inherent inefficiency of SDH/SONET rings by using statistical multiplexing, while providing a similar carrier-class service with respect to restorability/protection and versatile quality of service features. Another candidate for high-speed MAN is Gigabit Ethernet (GigE) which readily offers statistical multiplexing advantages but which lack measures for provisioning of fairness and fast restoration.

This paper provides an overview of the RPR protocol. The architecture of RPR-based networks and the main features of the protocol are outlined. Furthermore, we provide details on the physical and MAC layers of the protocol, automatic protection switching, and topology discovery. We also discuss possible ways and technologies that could be used by a carrier to evolve its services and network architecture to meet the ever-increasing demand for bandwidth in the metropolitan area.

2. DRIVERS FOR THE EVOLUTION OF METROPOLITAN-AREA NETWORKS

There is strong evidence that demand for more data-centric bandwidth in the metro area will increase during this decade. This stems from the fact of the changing nature of conducting business driven by new applications and the increased dependence on connectivity. The main drivers we see shaping this paradigm shift could be the following applications (This is not a conclusive list but has a good list of potential applications):

- Storage-Area Networks for large enterprises (and in particular financial institutions).
- Connecting service providers POPs with main POPs and Internet exchange points.
- High-speed transparent LAN interconnection.
- Campus interconnection and remote learning for educational institutions.
- Connecting enterprises with large data centers and hosting facilities.

3. OVERVIEW OF RESILIENT PACKET RINGS ARCHITECTURE

The main features of the RPR are as follows [2]:

- Efficient use of bandwidth using statistical multiplexing, spatial reuse, and small protocol overhead
- Support for three traffic priorities
- Scalability by allowing a large number of nodes to be connected to the ring
- Weighted fairness for bandwidth sharing among the nodes using the ring
- Support for ring-based redundancy and protection against failures similar to that found in SDH/SONET.
- Independence of the physical layer media type

We discuss how RPR can meet these objectives as we go through the details of the protocol.

3.1 Resilient Packet Rings Architecture

RPR uses a bi-directional ring consisting of two symmetric counter-rotating fiber rings as shown in *Figure 1*. One of the rings is called the “outer ring” whereas the other is called the “inner ring”. To reduce the amount of confusion, we refer to the outer and inner rings as the *ringlets*, while the whole ring composed of the two ringlets is referred to as the *ring*. The two ringlets can be simultaneously used for both traffic and control packets. A participate node operates by sending traffic packets in one direction (downstream) and sending the associated control packets in the opposite direction (upstream) on the other ringlet. The simultaneous use of the two fibers is a clear advantage for RPR over SDH/SONET rings where in SDH/SONEET one of the rings is fully dedicated for traffic protection.

RPR is based on using statistical multiplexing. No timeslot or dedicated bandwidth is allocated for (regular) traffic. By correctly dimensioning the network and forecasting the traffic demands, statistical multiplexing can offer orders-of-magnitude gains over TDM-based SDH/SONET rings.

We describe the operation of the RPR MAC protocol and how it provides fair access to the ring bandwidth in section 4.

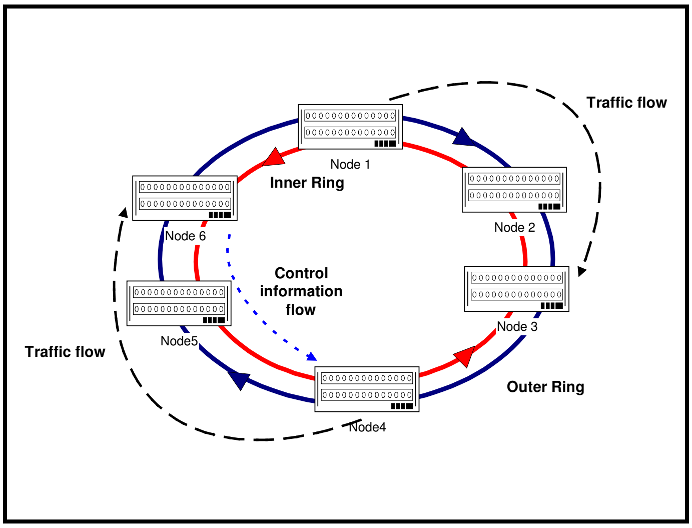


Figure 1. Architecture of RPR showing the spatial reuse feature

RPR defines three service classes for user traffic: class A or premium priority, class B or medium priority, and class C or low priority traffic. Class A is allocated with a committed information rate (CIR) and provides lowest end-to-end delay and jitter. Class B is allocated a certain CIR and provides bounded MAC delay and jitter for the amount of traffic within the profile on the CIR. Excess traffic above the CIR is referred to as excess information rate (EIR) class B traffic. Class C is mainly a “best-effort”/opportunistic service class that uses whatever remains of the network capacity. Class B EIR traffic is treated similarly to class C traffic. This traffic is subject to the distributed fairness operation of the RPR protocol and is marked as fairness-eligible (FE) traffic. Control traffic is usually sent as class A traffic.

An RPR node processes its own local traffic and transit traffic. Transit traffic is traffic not originating or terminating at the local node, in essence it is traffic generated at other nodes and passing through and RPR node on its way to the requested destination.

3.1.1 Transmit and Forwarding Operations

A simplified RPR node architecture is shown in . An RPR contains separate queues for the local and transit traffic. The queues handling the local traffic are named the transmit queues and the standard calls for three queues, one for each of the three classes. For transit traffic, there are two possible implementations. The first version uses two transit queues: a primary transit queue (PTQ) for class A transit traffic and a secondary transit queue (STQ) for classes B and C traffic. The second version implements a one transit queue for all types of transit traffic (which is also termed a PTQ in this case). In addition to the transmit and transit traffic queuing, all traffic is shaped/rate-controlled in order to maintain service class guarantees. However, no traffic shaping is applied to transit traffic at the PTQ.

The RPR MAC client can transmit packets from five possible queues in the dual-transit queue implementation and from four queues in the single-transit queue implementation. The RPR MAC decides on which queued frames to send next based on a priority scheme explained as follows.

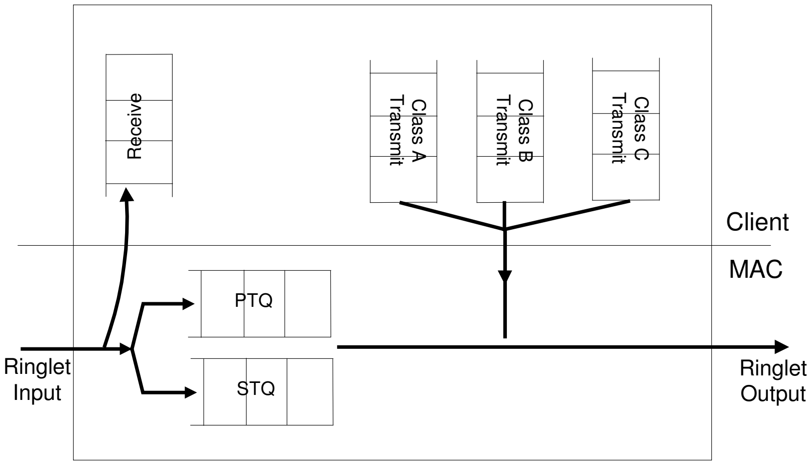


Figure 2. Simplified RPR node architecture with transit and transmit queues

In the dual-transit queue implementation, Class A transit traffic in the PTQ are always sent first. Class A local traffic may be sent as long as the STQ is not almost full (as determined by a certain threshold). Local class B traffic within CIR is sent next as long as the STQ is not almost full. Local EIR class B in the class B transmit queue and local class C traffic is sent next as long as they do not violate the fair share of the bandwidth and the STQ has not exceeded a low priority threshold. If nothing else can be sent, then traffic in the STQ can be sent.

In the single-transit queue implementation, transit traffic is always sent first. Local traffic will then be sent in the order class A, class B, and EIR class B and class C. EIR class B and class C traffic will be limited to the fair rate governed by the distributed RPR fairness protocol.

3.1.2 Spatial Reuse

In RPR, the MAC protocol operates in a destination-stripping mode. Previous data ring technologies such as FDDI or Token Ring was based in source stripping. In source stripping, packets circulate the whole ring until they return to the source where the packet is removed from the ring. In contrast, RPR uses destination stripping, where the destination removes the packet from the ring. The full ring bandwidth on other segments of the rings is available for use by other source destination pairs. This is illustrated in *Figure 1*, where the pair of nodes (1, 3) and (4,6) are simultaneously using the ring. The destination stripping is applied on unicast packets only. Other packets (broadcast or multicast) are stripped by the source. Depending on the traffic flow patterns, spatial reuse can offer high bandwidth gains.

3.2 RPR Physical Layer

A primary goal of the RPR standard is to be physical media independent. RPR can work over dark-fiber, WDM, SONET/SDH, or Gigabit Ethernet physical media.

The case of SDH/SONET physical media is particularly interesting. The standard defines operation over STM-4/OC-12, STM-16/OC-48, and STM-64/OC-192. The STM-4 and STM-16 operation are defined by the SPI-3 interface [5], while the STM-64 operation is defined by the SPI-4 interface [6], both defined by the Optical Internetworking Forum (OIF). RPR is mapped to a tributary connection of a SDH/SONET network via an ADD/Drop Multiplexer. The two RPR rings may be mapped to two STS-N connections. In this case, SDH/SONET provides layer 1 protection while RPR provides layer 2 protection. It is advisable to either delay the activation of RPR protection beyond 100 msec to allow for SDH/SONET level protection to occur, or to configure SDH/SONET without protection.

RPR can be mapped to a SDH/SONET payload using either Packet-Over-SDH (POS) framing [10] or using the Generic Framing Protocol (GFP) [8] framing.

4. THE RPR MEDIA ACCESS CONTROL PROTOCOL

4.1 Packet Format

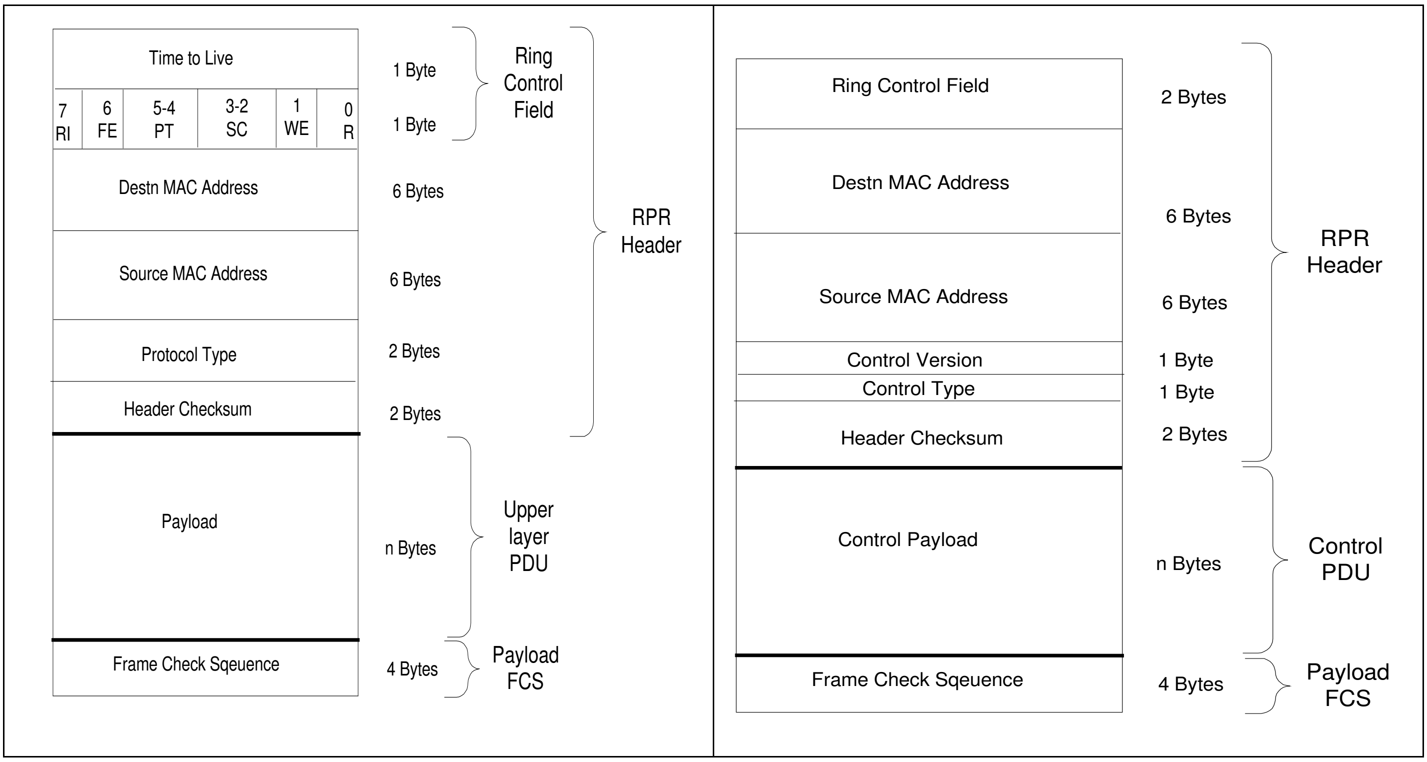


Figure 3. (a) RPR traffic packet format (b) control packet format

RPR packets can be sent over a variety of layer 1 transports such as SDH, Ethernet, POS, or GFP. The maximum transfer unit (MTU) is 9216 octets whereas the minimum transfer unit is 42 octets.

There are three main type of RPR packets: traffic, control, and usages packets. The structure of traffic and control packets is shown in *Figure 3*. Usage packets will be discussed in details in section 4.2.

All RPR packets have a common RPR header which consists of the following fields:

- Time To Live (TTL): This is an 8-bit hop count that must be decremented each time a node processes an incoming packet. If the value becomes zero, the packet is stripped off the ring. This allows for a maximum ring size of 256 nodes. However, due to ring wrapping in the case of failures, the actual number is 128 nodes.

- RI: This is a 1-bit field indicating on which ringlet was the frame originally transmitted.

- FE: This is a 1-bit field indicating whether the packet is eligible for the fairness protocol operation or not.

- PT: This is a 2-bit field which identifies the packet type as follows: 0 is reserved for future use, 1 is for control packets, 2 is for fairness (usage) packets, and 3 is for traffic packets.

- SC: This is a 2-bit field which indicates the service class of the packet (values 0 through 3 indicates traffic classes C, B, A1, A0 respectively).

- WE: This is a 1-bit field indicating whether the packet is wrap-eligible or not, i.e. whether at a wrap condition, the network can wrap the packet for protection or not.

- R: This is a 1-bit field that is reserved for future use.

- Destination and Source Address: These are 48-bit fields indicating the node to which the frame is intended and which originated the frame respectively. The address is the same as that defined for the IEEE 802 protocol family [4].

- The following two bytes are different in the case of traffic or control packet. For traffic packets, the two bytes denote the protocol type. This field is used as follows: if its value is greater than 1536, then it identifies the MAC client protocol, if less than 1536 then it identifies the length of the payload. For control packets, the first byte indicates the control version (which is initially 0) and the following byte identifies the type of the control packet (currently only topology discovery, protection, OAM types are defined).

- Header Error Check (HEC): This is a 16-bit error checking code computed over the RPR header, destination and source address, and the 2 bytes comprising the protocol type for traffic packets or the control version + control type for control packets.

Following the header, the packet contains a payload which is either user or control traffic. A frame check sequence comprised of 32-bit cyclic-redundancy check (CRC) field is added at the end of the RPR frame. This CRC is generated similarly to other IEEE 802 standard and is generated on what follows the header checksum, i.e. the payload.

4.2 Fairness Algorithm

Achieving fair bandwidth and resource sharing in a high-speed ring architecture covering typical distance spans in large metropolitan area is known to be a challenging problem [9]. Fairness is one of the most desirable attributes to exist in a MAC protocol working in such an environment. It is desirable that all nodes will have fair access to the available ring bandwidth independent of their location or their aggregate generated traffic. The RPR protocol designers realized this early on and several proposals were scrutinized by the working group to reach a good protocol design. The version presented here is the one outlined in the draft standard [2]. The bandwidth fairness provided by RPR which is claimed to be independent of node location and the heterogeneity of the traffic profiles of the nodes. This is one of the distinct advantages over other candidate technologies for packet based MANs such as Gigabit Ethernet.

The RPR fairness algorithm implements the following functions within the MAC layer:

- Determining when the congestion threshold is crossed and when the congestion has leveled off
- Determining the node's allowed rate
- Determining the fair rate for advertising fairness control messages (FCMs)
- Communicating the allowed rate to the traffic shapers for controlling access to the medium

To provide full details about the fairness algorithm would need many pages. We provide an overview of the operation and refer the interested reader to the standard documents for further details. The RPR MAC fairness algorithm is only applied fairness-eligible (FE) traffic: namely class C and class B excess traffic. Traffic class A and within limit class B with guaranteed CIR rates are not fairness-eligible and are provisioned by other means such as traffic engineering and network management. The available bandwidth to be used by FE traffic is the difference between link capacity and the reserved rate for the guaranteed traffic.

The fairness algorithm uses various counters, thresholds, and other parameters at each node to perform its job. Each node is assigned a weight which allows a network operator to assign more ring bandwidth to certain nodes as needed (in essence as contracted). Each node on the ring advertises a fair rate to upstream nodes via the opposite ringlet upon which the algorithm is running. There are two key variables measured at each node: *forwarded_rate* and *local_rate*. The first identifies the overall rate of transit traffic and the second identifies the rate of the own node traffic. The measured variables are run through a low-pass filter to prevent oscillations. The measured variables are updated periodically with a period length that is a function of the link rate of the ring.

Congestion at a particular node is detected if ANY of the following conditions become true:

- The overall rate of outgoing traffic exceeds the link capacity minus the reserved rate for non-fairness eligible traffic or exceeds the parameter *low_threshold.*

- The depth of the secondary transit queue (STQ) exceeds the *low_threshold* congestion depth threshold.

- The access delay timer for class B packets expires.

- The access delay timer for class C packets expires.

Periodically, a node sends a fairness control message (FCM) to upstream nodes to advertise its current value of the *local_rate* (normalized by node's weight, aging coefficient, and rate coefficient). The aging coefficient is used for aging the measured variables with default value of 4. The rate coefficient normalizes measured variables with respect to link speed (links with 2.5 Gpbs or lower rates have a coefficient of 1, 10-Gbps links have a coefficient of 4, and so on).

There are actually two types of FCM: Single Choke (SC-FCM) and Multi Choke (MC-FCM). The format of the FCM is shown in *Figure 4*. We note here that when the 3-bit field fairness message type has a value of 000 it indicates a SC-FCM while a value of 001 indicates a MC-FCM. The control value field actually contains the fair rate information encoded as a 16-bits quantity. A value of all 1's indicate a fair rate equal to full available link rate and is subsequently referred to as FULL_RATE.

Ring Control Field (PT=0x02)		2 Bytes
Source MAC Address		6 Bytes
Fairness Message Type (3 bits)	Reserved	1 Bytes
Reserved		1 Bytes
Control Value		2 Bytes
Frame Check Sqeuence		4 Bytes

Figure 4. Format of Fairness Control Message

SC-FCM are propagated hop-by-hop around the opposite ringlet and processed by the fairness control unit (FCU) of the respective MAC layer ar each node and are sent periodically. The rate at which the SC-FCM's are sent is adjustable with a parameter called *ADVERTISEMENT_INTERVAL* such that the overall bandwidth consumed by FCM does not exceed 0.125% of the available ring bandwidth at each node.

When an upstream nodes receive the SC-FCM with an advertised rate *rcvd_fair_rate*, they will adjust their rates to the minimum of the node's current rate and that received in the SC-FCM (as adjusted by the respective node weight). The node stores the values *rcvd_fair_rate* and the MAC address of the source available in the SC-FCM. Afterwards, when it is the node's term to send its SC-FCM, it either sends the message with the MAC address of the last received node or its own MAC address according to the algorithm in *Figure 5*.

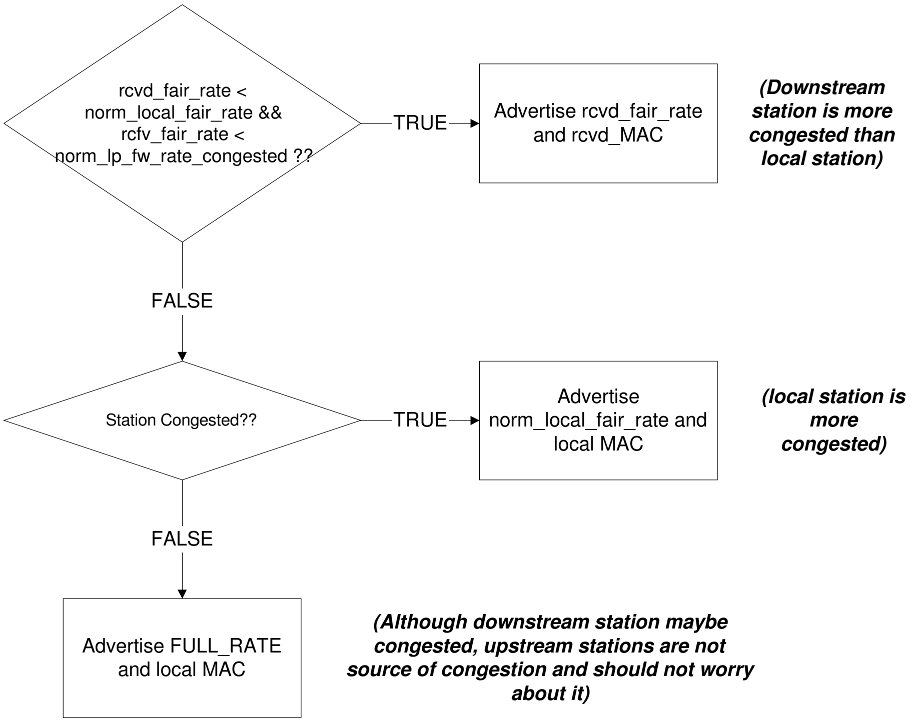

rcvd_fair_rate < norm_local_fair_rate && rcfv_fair_rate < norm_lp_fw_rate_congested ??
TRUE
Advertise rcvd_fair_rate and rcvd_MAC
(Downstream station is more congested than local station)
FALSE
Station Congested??
TRUE
Advertise norm_local_fair_rate and local MAC
(local station is more congested)
FALSE
Advertise FULL_RATE and local MAC
(Although downstream station maybe congested, upstream stations are not source of congestion and should not worry about it)

Figure 5. Single Choke Message Advertising and Handling

MC-FCMs are broadcast on the opposite ring and contains the MAC address of the node that originated the message. The MC-FCMs are sent at one-tenth the rate of SC-FCM and are not processed by the FCU. If a node experiences congestion it will send its *local_fair_rate* or otherwise the *FULL_RATE* value is sent. The received MC-FCM are passed by the FCU to the MAC client which can use the information contained in the MC-FCM to perform virtual destination queueing (VDQ). VDQ is used to increase throughput by allowing a node to send traffic to a destination that happens to be before the congested link at a higher rate than nodes after or at the congestion point.

The proposed RPR fairness protocol is far from being perfect. It mainly suffers from instability and oscillations of the allowed fair rates and slow convergence. It also suffers from relatively long MAC delays for best effort traffic due to high occupancy of the transit buffers as evidenced by the results of [7] [11]. Another drawback is that "parameter setting requires experience and a crystal ball" [11].

Many efforts and alternative proposals are being discussed. We mention here the work on Distributed Virtual-time Scheduling in Rings (DVSR) [7] and a proposal by the IKN group of the Technical University of Vienna [11] as good candidates. The work by [11] is based on cyclic reservations and has historical links to the CRMA protocol [12]. This does not seem to be compatible with current RPR standard proposal. DVSR has the advantage of being compatible with current RPR fairness mechanisms and can be implemented within RPR.

4.3 Intelligent Protection Switching

One of the main features of the RPR protocol is providing mechanisms for resiliency. The RPR protection protocol provides reliable mechanisms for sub-50 ms protection switching for protected traffic on an RPR. It is comprised of two schemes: a mandatory mechanism called steering, and an optional mechanism called wrapping. The protection mechanisms defined for RPR are quite strong in the following sense: they are independent of the existence of a management node, operate without any master node on the ring, scalable from 1 to hundreds of nodes, and support dynamic removal and addition of nodes.

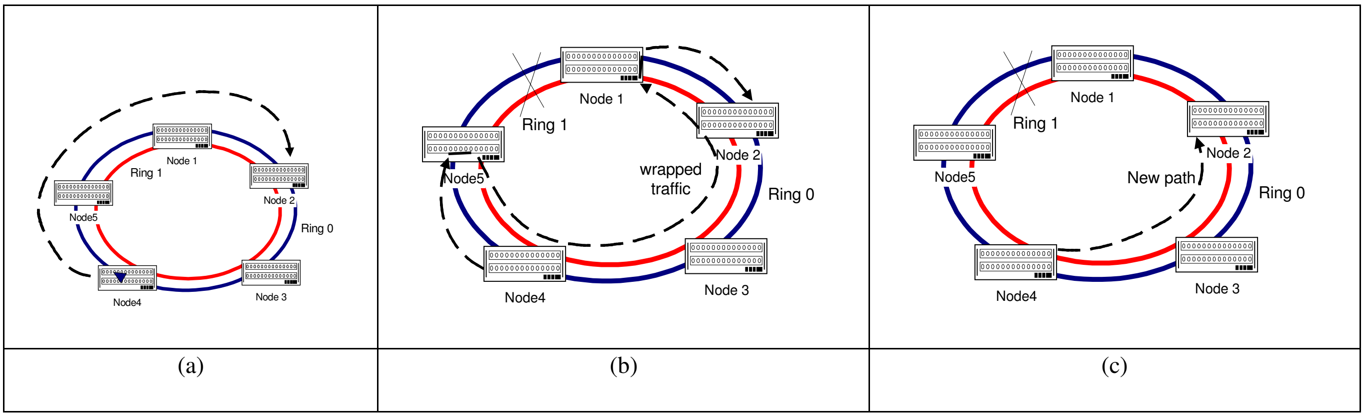
4.3.1 Steering Protection

In steering protection, when a node detects a failure, it broadcasts a protection request message (PRM) to all nodes to indicate a link or node failure. The nodes receiving the PRM will update their steering database accordingly. Afterwards, the traffic is directed to either ringlet or ringlet 1, whichever avoids the location of the failure. Traffic reaching the node detecting the failure and destined to a node beyond the point of failure will be dropped.

4.3.2 Wrap Protection

In wrap protection, it is assumed that the RPR ring consists of two counter-rotating ringlets. If a link or node failure is detected, traffic going towards the failure is wrapped back to go in the opposite direction on the other ring.

For example, consider the 5 node ring shown in *Figure 6*. Before the fiber cut node 4 send to node 2 via the path $4 \xrightarrow{0} 5 \xrightarrow{0} 1 \xrightarrow{0} 2$ on ringlet 0 (the number above the arrow is ringlet id). When a fiber cut occurs between node 5 and 1, a wrapping of the traffic occurs and the traffic between 5 and 1 goes through ringlet 1. So, initially after wrapping the traffic between 4 and 2 will follow the path $4\xrightarrow{0}5\xrightarrow{1}4\xrightarrow{1}3\xrightarrow{1}2\xrightarrow{1}1\xrightarrow{0}2$ (part b of the graph), which is not optimal. Subsequently, the topology discovery mechanism will find out that the best path for communication between 4 and 2 is $4\xrightarrow{1}3\xrightarrow{1}2$ (part c of the graph). It is to be noted here that wrapping is controlled through an SDH/SONET-like BLSR signalling messages.



(a) (b) (c)

Figure 6. Example showing wrap protection operation. (a) Normal flow before fiber cut (b) Flow after fiber cut showing wrapped traffic (c) Optimized flow after next topology discovery

4.3.3 Protection Message Format

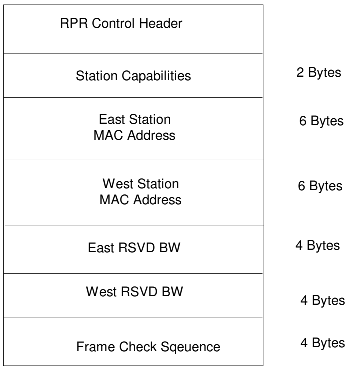
RPR Control Header					
7 RSVD	6 WSC	5 RSVD	4 PI	3-0 PMRT	1 Bytes
Sequence Number					1 Byte
Frame Check Sqeuence					4 Bytes

Figure 7. Format of Protection Message

The protection message is used for signaling link failures and degradations. The protection message packet format is shown in *FIGURE 7*. Within the header, the source address contains the address of the node discovering the failure, and the destination address is the broadcast addresses on the ring. The following byte after the control header contains 3 fields. Bit 6 is the wrapping status code (WSC) bit which indicates whether a node has completed wrapping or not (1 for completing, 0 for idle). Bit 4 is the path indicator (PI) bit which indicates whether the path (over which the protection message is sent) is long 1 or short 0. Bits 0 to 3 are called the protection message request type (PMRT), which define five types of requests and an idle request type. Bits 5 and 7 are not used. The following byte is a sequence number byte containing the message sequence number which is used for the two copies of the protection message sent on the two ringlets. The sequence number is incremented after each transmission of a protection message. The purpose is that no message will be processed twice by a node receiving the two copies of the message on the inner and outer ringlets.

4.4 Topology Discovery

An important operation in RPR is topology discovery. The topology of the ring is not fixed. Nodes can join and leave the ring dynamically. The topology map also changes when failure are detected and isolated. The topology discovery protocol provides each node on the ring with knowledge of the number, arrangement and status of other nodes on the ring. This process is done periodically to reflect the dynamic changes that occur on the ring. Moreover, the protocol is fully distributed and all nodes assume the same role with regards to the protocol operation. No single node acts as a master for the topology information and a fully connected ring is not needed for proper operation of the protocol.



RPR Control Header	
Station Capabilities	2 Bytes
East Station MAC Address	6 Bytes
West Station MAC Address	6 Bytes
East RSVD BW	4 Bytes
West RSVD BW	4 Bytes
Frame Check Sqeuence	4 Bytes

Figure 8. Format of the topology discovery message

All topology discovery operations are carried out via topology discovery messages carried within an RPR control packet with control type value of 1. These messages are sent as broadcast frames on all ringlets, with a TTL value of 255 and are removed by the source node. The topology discovery message format is shown in *Figure 8*.

Within the topology discovery message, the node capabilities field is comprised of two bytes containing information about node capabilities: for example its weight as when applying the fairness protocol and its wrap-protection capability. The frame contains the MAC address of the neighbouring east and west nodes. If these addresses are not known (for example when a node is booted or inserted into the ring), their values are set to 0. The reserved bandwidth denotes the total bandwidth reserved for class A traffic on the incoming link to the east and west of the incoming links to the node.

The topology discovery messages are generated on the initial startup of node, when a node detects a failure or a change in local status (for example reserved bandwidth), when it detects a new node on the ring, and also periodically with a period configurable from 128 to 1024 milliseconds.

When a topology message is received by a node it processes it as follows. If the message is not received on the same ringlet over which it was sent, the message is discarded (and detects a mis-cabling error), otherwise it is accepted and the receiving node uses the information in the message to update its topology database. If the received message is received from a direct neighbour the receiving node will validate and update if needed the identity of its neighbour.

During protection switching, the topology messages are not wrapped and shall be stripped. Therefore all topology discovery messages must have a WE bit set to zero.

5. DISCUSSION & CONCLUSIONS

RPR is a new evolving standard for constructing packet-based scalable ring architecture for use by the bandwidth-hungry applications expected to proliferate into metropolitan area networks. The technology couples the efficiency and simplicity of packet-based Ethernet with the strong protection capabilities of the TDM-based SDH/SONET rings. The main advantage over SDH/SONET rings are the cost-effectiveness and the bandwidth efficiency. RPR also provide means for bandwidth guaranteed connections similar to SDH point-to-point circuit-switched connections. A competing technology in this domain is Gigabit Ethernet. However, the advantages of RPR over GigE are clear: the fairness and sub-50 msec protection which are not well-defined for GigE. The RPR fairness protocol strives to achieve location-independent fairness and prevents hogging available bandwidth by few users. Another important feature of RPR is spatial reuse, which causes bandwidth to be used efficiently on the ring in case the traffic profile allows the reuse.

It remains to be seen whether carriers and operators should switch to this new technology or upgrade existing SONET/SDH equipment. SDH rings can be enhanced via grooming devices at the edge which can offer statistical multiplexing gains and also by allowing more dynamic establishment and release of TDM connections. In many circumstances, a new technology is not always necessary to be deployed. Any operator must therefore carry out a detailed study of the services needed in a specific area, the projected traffic demand and its nature, and the cost tradeoffs between new equipment deployment, upgrade of existing equipment and how much customers are willing to pay for best-effort traffic versus guaranteed TDM-like connections. In essence, there would be no single universal solution for every case. We also predict strong competition from networks constructed using less expensive Gigabit Ethernet switches where current effort is directed towards enhancing the standard spanning-tree protocol to offer fast restoration in case of failures or topology updates [1]. Also, simplicity of gigabit Ethernet is an extremely attractive property.

REFERENCES

[1] Extreme Network, Ethernet Automatic Protection Switching, available from http://www.extremenetworks.com/libraries/prodpdfs/products/extware.pdf

[2] IEEE Draft Standard 802.17/D.10 for Resilient Packet Rings (RPR), August 2002.

[3] IEEE Standard 802.6 Distributed Queue Dual Bus (DQDB) Access method and physical layer specifications, 1994.

[4] IEEE Standard 802-2001 for Local and Metropolitan Area Networks: Overview and Architecture, 2001.

[5] Optical Internetworking Forum Standard OIF-SPI3-01.0, System Packet Interface Level 3 (SPI-3): OC-48 System Interface for Physical and Link Layer Devices.

[6] Optical Internetworking Forum Standard OIF-SPI4-02.0, System Packet Interface Level 4 (SPI-4) phase 2: OC-192 System Interface for Physical and Link Layer Devices.

[7] V. Gambiroza, Y. Liu, P. Yuan, and E. Knightly, `High-Performance Fair Bandwidth Allocation for Resilient Packet Rings, in Proceedings of the 15th ITC Specialist Seminar on Internet Traffic Engineering and Traffic Management, Wurzburg, Germany, July 2002.

[8] S. Gorshe and T. Wilson, Transparent generic framing procedure (GFP): A protocol for efficient transport of block-coded data through SONET/SDH networks, IEEE Communications Magazine, pp. 88-95, May 2002 .

[9] E. Hahne, A. Choudhury, and N. Maxemchuk, DQDB Networks with and without Bandwidth Balancing, IEEE Transactions on Communications, pp. 1192-1204, July 1992.

[10] A. Malis and W. Simpson, PPP over SONET/SDH, IETF RFC 2615, 1999.

[11] Harmen R. van As and Roman Morawek. Distributed Resource Reservation for RPR. Presentation in the IEEE 802.17 Resilient Packet Ring Working Group. September 2001. Available from http://grouper.ieee.org/groups/802/17/documents/presentations/sep2001/vas_perfo_01.pdf

[12] M. Nassehi, CRMA: an access mechanism for high speed MANs and LANs, in Proc. IEEE ICC'90, pp. 345.5.1-345.5.6, 1990.

[13] W. Willinger, M. S. Taqqu, R. Sherman, D. V. Wilson, Self-similarity through high-variability: Statistical analysis of Ethernet LAN traffic at the source level, IEEE/ACM Transactions on Networking, no. 1, pp. 71-86, Feb 1997.