Outline of the IEEE 802.17 RPR Draft Standard

Version 0.3

An Overview by the
Resilient Packet Ring Alliance
June 2002

Outline of the IEEE 802.17 RPR Draft Standard
Version 0.3

The IEEE 802.17 Resilient Packet Ring (RPR) standard draft defines a media access control (MAC) layer for metropolitan area ring networks. Broadly speaking, the draft includes the following:

- A MAC reference model that identifies the relevant components of the MAC and their relationship to one another as well as protocol layers below and above the MAC in the standard OSI reference model
- A description of the MAC itself, which includes the access control protocol, the data path, as well as frame formats for data and control frames
- A protection switching protocol that enables the detection of faults and subsequent restoration of services on the ring within 50 msecs
- A topology discovery protocol
- Network management primitives that enable administration and management of the RPR MAC

MAC Reference Model

The reference model identifies the various sub-components of the MAC and their relationship to each other. The model also defines the control and data interface between the MAC and the MAC client and between the MAC and PHY layers.

The RPR MAC provides support for three different types of services.

- High: The high priority service supports applications that require bandwidth guarantees and tightly bounded delay and jitter specifications. Examples include voice, video, and circuit emulation applications. Bandwidth can be reserved for high priority services, ensuring this bandwidth will not be reclaimed by lower priority services when idle.
- Medium: The medium priority service supports applications that are not very sensitive to delay but still require a bandwidth commitment. Examples include CIR (constant information rate) data applications. Bandwidth committed to a medium priority service is reclaimable – idle bandwidth will be available to active medium and low priority traffic on the ring.
- Low: The low priority service supports best-effort data traffic. Low priority services have no reserved bandwidth committed to them – they always receive their fair share of any unused capacity on the ring.

Media Access Control (MAC)

There are several components to the MAC specification including the data path, the access control protocol, and the frame format.

MAC Data Path

The MAC data path section describes the handling of data traffic in the MAC. The RPR MAC on a station needs to process two types of data traffic: ingress traffic being sent by the MAC client for transmission on the ring and transit traffic coming from the upstream neighbor on the ring meant for some node downstream on the ring. The RPR MAC supports two transit path implementations: a single buffer implementation that always prioritizes transit traffic over ingress traffic and a dual buffer implementation that separates low priority and high priority transit traffic with the MAC scheduling transmission of frames from the ingress transit queues.

MAC Fairness

The MAC fairness section defines the access control protocol that ensures fair access to ring resources. The RPR MAC includes mechanisms for detecting the level of congestion on any link in the ring. Each MAC monitors the utilization of the links it is attached to. Other nodes on the ring are informed of what their fair share of the congested link is. The MAC in each node is then responsible for limiting ingress traffic to that fair rate.

Frame Format

The frame format section of the draft defines the frame format for all RPR frames. The MAC frame header includes a 2-byte RPR header, the destination and source MAC address, a protocol type field and a HEC field for header error checking. (See Figure 1 for details.)

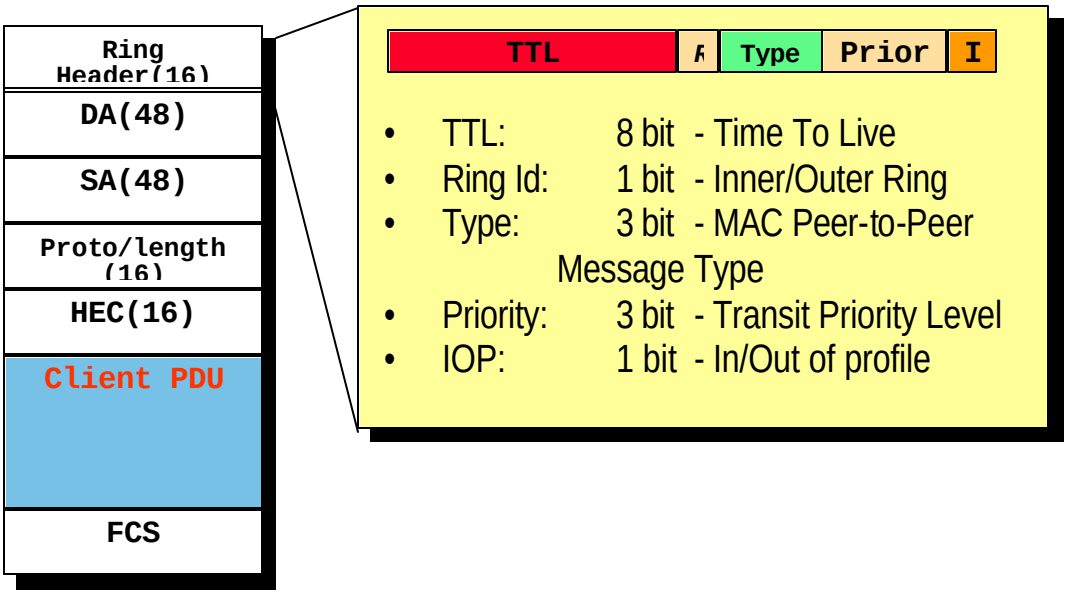

Figure 1. RPR Frame Format

MAC Physical Interface

This section specifies reconciliation sublayers that enable the MAC to interface with existing physical (PHY) layers. The reconciliation sublayer plays an important role in making the RPR MAC PHY layer-agnostic. It maps the logical MAC physical layer service primitives to and from standard electrical interfaces used by the physical layers.

The standard specifies reconciliation sublayers for Ethernet and SONET/SDH.

Two Ethernet reconciliation sublayers are defined in the draft:

1. The gigabit Ethernet reconciliation sublayer (GERS) provides a standard interface for use with gigabit Ethernet PHYs.
2. The ten-gigabit (10G) Ethernet reconciliation sublayer (XGERS) provides a standard interface for use with ten gigabit Ethernet PHYs.

Ethernet PHYs supported by the 802.17 standard include:

- Gigabit Ethernet PHYs: 1000BASE-SX, 1000BASE-LX
- 10G LAN PHYs: 10GBASE-SR, 10GBASE-LR, 10GBASE-ER, 10GBASE-LX4
- 10G WAN PHYs: 10GBASE-SW, 10GBASE-LW, 10GBASE-EW

Two SONET/SDH reconciliation sublayers are also defined in the draft:

1. The SONET/SDH reconciliation sublayer (SRS) can be used with a GFP or HDLC-like framing adaptation sublayer
2. The GFP reconciliation sublayer (GRS) can be used with the GFP adaptation sublayer

Both types of reconciliation sublayers are specified with 8-bit SPI-3, 32 bit SPI-3, SPI-4.1, and SPI-4.2 interfaces operating at various speeds.

Protection

The RPR MAC supports two protection mechanisms: wrapping and steering. Each mechanism has its advantages, and support for both ensures that service providers can optimize their networks according to the particulars of the application.

In wrap protection, if an equipment or fiber facility failure is detected on a span, traffic going towards the failure is wrapped (or looped) back in the opposite direction. Wrapping takes place on the stations adjacent to the failure, under the control of the protection switch protocol controlled by the MAC. The wrap essentially re-routes the traffic away from the failure as shown in Figure 2.

For steer protection, a station will not wrap a failed ring segment when a failure is detected. Instead, all stations are constantly kept aware of the status of each link and, in the event of a failure, will "steer" traffic away from the failure. Source stations thus retain the responsibility of directing traffic onto the appropriate ring, the one that avoids the failure. (This scenario is also shown in Figure 2.)

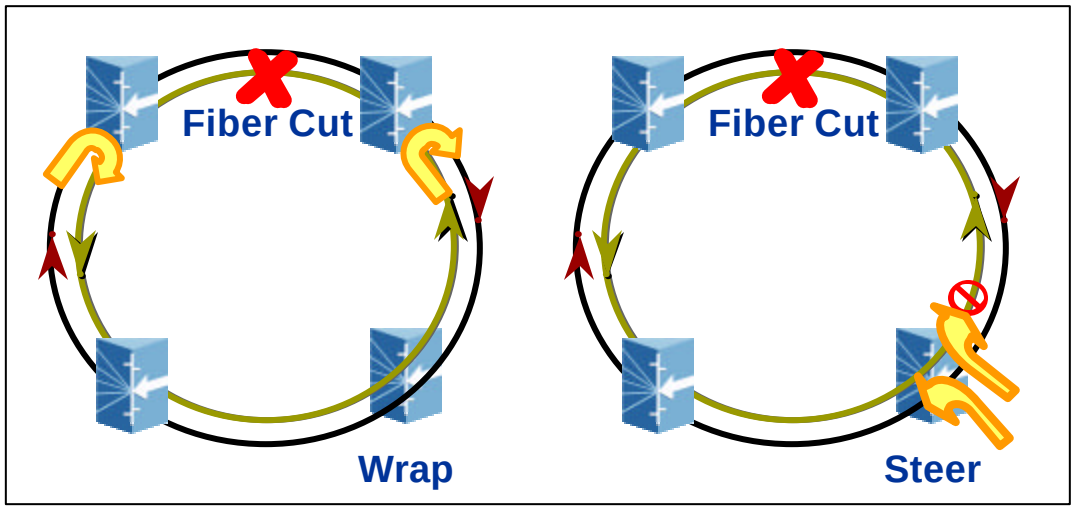

Figure 2. Wrap and Steer Protection in RPR

Steering is the default protection mechanism in the current proposed RPR standard. This means that when an RPR ring contains stations that can both wrap and steer, they will default to steer protection to ensure interoperability.

Topology Discovery

This section describes the RPR topology discovery protocol, which implements a reliable and accurate means for all RPR stations on a ring to discover the initial topology of the stations on the ring and any changes to that topology.

The RPR topology discovery protocol provides each station on the ring with knowledge of the number and relative position of other stations on the ring. Ring topology discovery is initiated as needed and periodically. This is a fully distributed protocol – no station acts as a master for the topology image or for the protocol. In addition to station identifiers and physical connectivity relationships, the topology discovery protocol is also used to propagate additional station information, for use in other parts of this standard.

Operations Administration Maintenance (OAM)

This section defines the management primitives for the RPR MAC. Management functional areas relevant to the RPR MAC include fault management, configuration management, and performance management. This section also describes the alarm signals and fault localization tools supported by the RPR MAC.

About the Resilient Packet Ring Alliance

The RPR Alliance, founded in January 2001, is an industry advocacy group committed to the development of an RPR technology standard for the networking industry. The Alliance will promote the adoption of an RPR standard for LANs, MANs, and WANs by educating the networking industry about RPR technology and the benefits of an IEEE standard as well as by fostering multi-vendor interoperability. Principal members of the RPR Alliance include Alcatel, Alidian Networks, Cisco Systems, Corrigent Systems, Lantern Communications, Mindspeed Technologies, Nortel Networks, and Vitesse Semiconductor Corporation. ARRIS, Avaya Communication, Chip Engines, Huawei Tech Co., Infineon Technologies, Intel, Ixia, NEC Corporation, Xilinx, and ZTE Corporation are participating members in the Alliance. For more information about the Alliance and the membership application, see www.RPRAlliance.org.