# Resilient Packet Ring Networks

## Definition

Resilient packet ring (RPR) technology is optimized for robust and efficient packet networking over a fiber ring topology. This technology incorporates extensive performance monitoring, proactive network restoration, and flexible deployment capabilities. RPR networks have the ability to carry multiple services, including jitter- and latency-sensitive traffic such as voice and video in addition to Ethernet and Internet protocol (IP) services. RPR combines the best features of legacy synchronous optical network (SONET)/synchronous digital hierarchy (SDH) and Ethernet into one layer to maximize profitability while delivering carrier-class service.

## Overview

RPR networks are optimized to transport data traffic rather than circuit-based traffic. This packet transport, with bandwidth consumed only between source and destination nodes, is more efficient than a time division multiplexing (TDM) transport such as SONET/SDH. RPR also offers the ability to differentiate and provide improved service for jitter- and latency-sensitive traffic on the ring.

Service providers and enterprise customers seek RPR solutions to deliver multiple services, instead of having data, voice, and video delivered over separate parallel networks. RPR has the unique advantage of delivering efficient data transport with the resiliency and performance required by the most demanding applications. This converged network offers service providers a path to new profitable services and offers enterprise customers a more efficient network infrastructure. Both service providers and enterprise customers benefit from the improved scalability and the ease of management of RPR networks.

Initial RPR products based on IETF RFC 2892—spatial reuse protocol (SRP)—have been deployed in networks worldwide. The IEEE 802.17 working group is currently defining an industry standard for an RPR media access control (MAC). This paper will detail the benefits and basic operation of RPR networks focusing on the proposed IEEE 802.17 implementation.

## Topics



# 1. Introduction

Service providers and enterprises are meeting customer demand by building scalable, feature-rich networks that can deliver profitable value-added services such as multiprotocol label switching (MPLS) virtual private networks (VPNs); voice, video, and data integration; and tiered service offerings. These services must be deployed with uncompromised reliability and scalability. To be economically and operationally feasible, this network must reduce the layers of equipment and management versus services offered over multiple parallel networks.

Data, rather than voice circuits, dominates today's bandwidth requirements. New services such as IP VPN, voice over IP (VoIP), and digital video are no longer confined within the corporate local-area network (LAN). These applications are placing new requirements on metropolitan-area network (MAN) and wide-area network (WAN) transport. RPR is uniquely positioned to fulfill these bandwidth and feature requirements as networks transition from circuit-dominated to packet-optimized infrastructures.

**Table 1. Resilient Packet Ring Technology Key Features**

| | |
|---|---|
| **Resilience** | Proactive span protection automatically avoids failed spans within 50 ms. |
| **Services** | Support for latency/jitter sensitive traffic such as voice and video.Support for committed information rate (CIR) services. |
| **Efficiency** | Spatial reuse: Unlike SONET/SDH, bandwidth is consumed only between the source and destination nodes. Packets are removed at their destination, leaving this bandwidth available to downstream nodes on the ring. |
| **Scalable** | Supports topologies of more than 100 nodes per ring. Automatic topology discovery mechanism. |

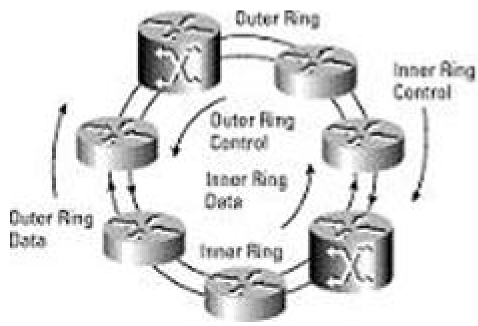
Service providers worldwide, such as cable multiple-system operators (MSOs), Internet service providers (ISPs), exchange-point operators, and Post Telephone and Telegraph Administrations (PTTs), have deployed current RPR solutions from companies such as Cisco Systems, Nortel Networks, and Sun Microsystems. The SRP, defined in IETF RFC 2892, is the most widely deployed solution today, with products from a multitude of companies and more than 200 customers worldwide.

The IEEE is currently defining the standard for a RPR MAC in the 802.17 working group. Completion of the IEEE standard is expected mid-2003.

## 2. RPR Operation

RPR technology uses a dual counter rotating fiber ring topology. Both rings (inner and outer) are used to transport working traffic between nodes. By utilizing both fibers, instead of keeping a spare fiber for protection, RPR utilizes the total available ring bandwidth. These fibers or ringlets are also used to carry control (topology updates, protection, and bandwidth control) messages. Control messages flow in the opposite direction of the traffic that they represent. For instance, outer-ring traffic-control information is carried on the inner ring to upstream nodes.

**Figure 1. RPR Terminology**

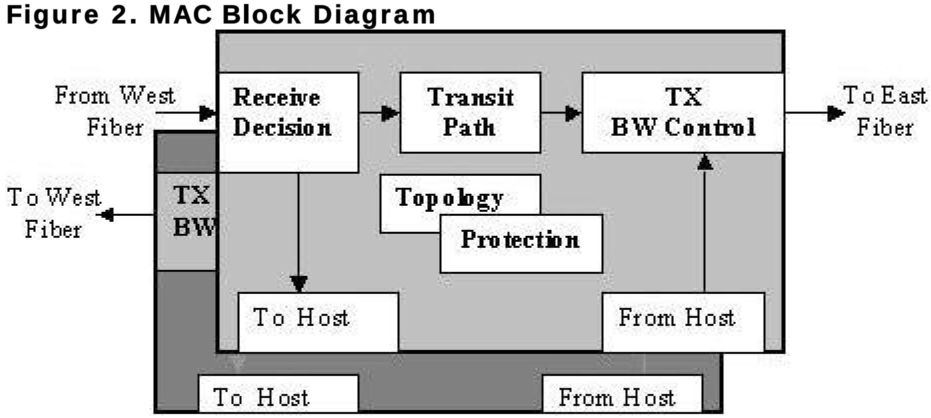



By using bandwidth-control messages, a RPR node can dynamically negotiate for bandwidth with the other nodes on the ring. RPR has the ability to differentiate between low- and high-priority packets. Just like other quality of service (QoS)–aware systems, nodes have the ability to transmit high-priority packets before those of low priority. In addition, RPR nodes also have a transit path, through which packets destined to downstream nodes on the ring flow. With a transit buffer capable of holding multiple packets, RPR nodes have the ability to transmit higher-priority packets while temporarily holding other lower-priority packets in the transit buffer. Nodes with smaller transit buffers can use bandwidth-control messages to ensure that bandwidth reserved for high-priority services stays available.

## The RPR MAC

As a Layer-2 network protocol, the MAC layer contains much of the functionality for the RPR network. The RPR MAC is responsible for providing access to the fiber media. The RPR MAC can receive, transit, and transmit packets.

**Figure 2. MAC Block Diagram**



**Receive Decision** – Every station has a 48-bit MAC address. The MAC will receive any packets with a matching destination address. The MAC can receive both unicast and multicast packets. Multicast packets are copied to the host and allowed to continue through the transit path. Matching unicast packets are stripped from the ring and do not consume bandwidth on downstream spans. There are also control packets that are meant for the neighboring node; these packets do not need a destination or source address.

**Transit Path** – Nodes with a non-matching destination address are allowed to continue circulating around the ring. Unlike point-to-point protocols such as Ethernet, RPR packets undergo minimal processing per hop on a ring. RPR packets are only inspected for a matching address and header errors (TTL=0, Parity, CRC).

**Transmit and Bandwidth Control** – The RPR MAC can transmit both high- and low-priority packets. The bandwidth algorithm controls whether a node is within its negotiated bandwidth allotment for low-priority packets. High-priority packets are not subject to the bandwidth-control algorithm.

The bandwidth-control algorithm dynamically negotiates available bandwidth between the nodes on the ring. This applies only to the low-priority service. It ensures that nodes will not be disadvantaged because of ring location or changing traffic patterns. The algorithm only manages congestion, enabling nodes to maximize the use of any spare capacity. Nodes can be inserted or removed from the ring without any bandwidth provisioning by the host.

## Topology Discovery

RPR has a topology discovery mechanism that allows nodes on the ring to be inserted/removed without manual management intervention. After a node joins a ring, it will circulate a topology discovery message to learn the MAC addresses of the other stations. Nodes also send these messages periodically (1 to 10 seconds). Each node that receives a topology message appends its MAC address and passes it to its neighbor. Eventually, the packet returns to its source with a topology map (list of addresses) of the ring.

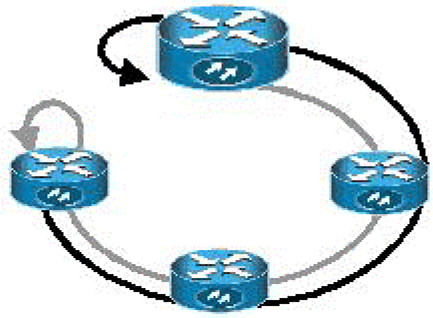
Routers are able to use the address resolution protocol (ARP) mechanism to determine which RPR MAC address belongs to the destination address of an IP packet. RPR switches and bridges will have a list of stations that they can reach through a RPR MAC address. The topology map will be used to determine which direction on the ring will provide the best path to the destination.

## Protection

RPR has the ability to protect the network from single span (node or fiber) failures. When a failure occurs, protection messages are quickly dispatched. RPR has two protection mechanisms:

**Wrapping** – Nodes neighboring the failed span will direct packets away from the failure by wrapping traffic around to the other fiber (ringlet). This mechanism requires that only two nodes participate in the protection event. Other nodes on the ring can send traffic as normal.

**Figure 3. Wrapped Traffic Flow**



**Steering** – The protection mechanism notifies all nodes on the ring of the failed span. Every node on the ring will adjust their topology maps to avoid this span.

Regardless of the protection mechanism used, the ring will be protected within 50 ms.

## Physical Layer

RPR packets can be transported over both SONET and Ethernet physical layers. The SONET/SDH physical layer offers robust error and performance monitoring. RPR packets can be encapsulated within the synchronous payload envelope (SPE) using a high-level data-link control (HDLC)–like or generic framing protocol (GFP) encapsulation. A robust Layer-1 protocol, SONET/SDH provides information such as loss of signal and signal degrade for use by the RPR protection mechanism. When using a SONET/SDH physical layer, RPR can be carried over SONET/SDH TDM transport or dark fiber.

Ethernet provides an economical physical layer for RPR networks. RPR packets are transmitted with the required inter-packet gap (IPG).

RPR Systems using the SONET physical layer will not interoperate with Ethernet physical-layer-based systems on the same ring.

# 3. Comparing RPR to Other Solutions

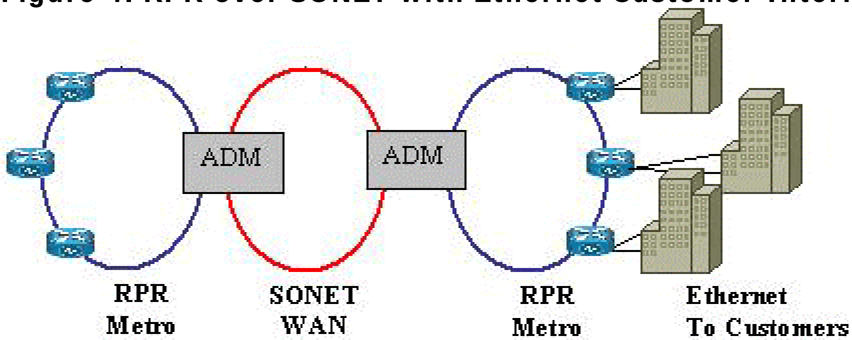
**Table 2. Comparing RPR to Other Solutions**

| | |
|---|---|
| **Legacy TDM** | Statically provisioned circuits<br>SONET/SDH limit of 16 nodes<br>Multiple layers of equipment for IP services |
| **Meshed Ethernet** | Spanning tree protocol (STP) limits protection response to minutes<br>Limited number of nodes<br>QoS applied at every hop |
| **Ethernet Rings** | Limited and proprietary protection schemes<br>Limited number of nodes<br>Packets are processed at each hop<br>No high-priority transit path |

# 4. Using RPR with SONET and Ethernet

Ethernet is the most common interface within enterprise networks. Although the optimal customer interface and LAN solution, Ethernet does not work well within metro networks. Most RPR edge systems offer an Ethernet interface as the customer interface. SONET/SDH can be used to transport RPRs that use the SONET/SDH physical layer. A 2.5G RPR can be carried as two optical carrier (OC)–48/synchronous transfer mode (STM)–16 channels (inner and outer rings) inside an OC–192/STM–64 SONET/SDH ring. This allows customers to utilize their existing transport infrastructure to deliver legacy TDM services, while RPR delivers data services efficiently. New SONET advancements such as virtual concatenation and the link-capacity adjustment scheme (LCAS) allow more precise and dynamic allocation of bandwidth dedicated to RPR services.

**Figure 4. RPR over SONET with Ethernet Customer Interfaces**

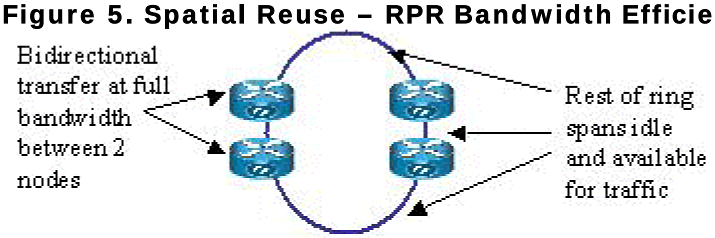



# 5. RPR Benefits

## Efficiency

- **Multicast** – One RPR multicast packet is transmitted around the ring and can be received by multiple nodes. Mesh topologies require multicast packets to be replicated over all possible paths, wasting bandwidth.
- **Spatial Reuse** – RPR unicast packets are stripped at their destination. Unlike SONET/SDH networks, where circuits consume bandwidth around the whole ring, RPR allows bandwidth to be used on multiple idle spans.

**Figure 5. Spatial Reuse – RPR Bandwidth Efficiency**




## Resiliency

- **Topology Discovery** – Nodes are automatically added and removed from the topology map.
- **Protection** – RPR protects failed spans within 50 ms.

### Performance

- **High-Priority Service** – High-priority packets are delivered with minimal jitter and latency.
- **Reliable** – RPR offers a lossless transport; nodes on the ring will not drop packets.

## 6. RPR Market Development

### ISP Networks

Without barriers of traditional SONET/SDH infrastructures, RPR solutions are helping ISPs to deliver reliable Internet services (such and IP and video) and address the growing bandwidth service requirements for the next-generation intra-point of presence (POP), exchange point, and server farm/storage applications.

### Regional Metro Networks

RPR enables regional metro networks designed to deliver Internet services (such as IP, VoIP, and video) to the metro. RPR regional metro solutions are available for transport over dark fiber, over wavelength division multiplexing (WDM), and over SONET/SDH, cable MSO, and enterprise/campus MANs.

### Metro Access Networks

RPR enables metro access solutions for service providers looking to deliver Internet services (such as IP, VoIP, and VPN) to metro access networks with direct Ethernet connectivity for multi-tenant/multidwelling customers and edge programmability.

## 7. Standardization

The IEEE 802.17 working group is working on the industry standard for an RPR MAC. This group was formed in January 2001 and expects to complete the standard in mid-2003.

## 8. The Future of RPR

RPRs provide a reliable, efficient, and service-aware transport for both enterprise and service-provider networks. Combining the best features of legacy SONET/SDH and Ethernet into one layer, RPR maximizes profitability while delivering carrier-class service. RPR will enable the convergence of voice, video, and data services transport.

## Self-Test

1. Resilient packet rings are transported over a ________ topology.

    a. Dual fiber

    b. Dual copper

    c. Wireless

    d. Laser

2. Resilient packet rings carry multiple services except _________.

    a. Internet Data

    b. Voice over IP

    c. Native TDM

    d. Packetized TDM

3. Jitter- and latency-sensitive traffic uses the _______ of RPRs.

    a. Normal service

    b. Bandwidth-control information

    c. High-priority service

    d. Control information

4. The IEEE standard for RPRs is ________.

   a. 802.1

   b. 802.3

   c. 802.16

   d. 802.17

5. When using the same physical layer, RPR can be transported within existing _______ networks.

   a. SONET/SDH

   b. ATM

   c. Token-ring

   d. Ethernet

6. A RPR node finds the other nodes on the ring via ________.

   a. Operator provisioning

   b. Automatic topology discovery

   c. Master topology list distribution

   d. Broadcast

7. A single fault on a RPR ring will be protected within _______.

   a. 10 seconds

   b. 100 ms

   c. 50 us

   d. 50 ms

8. To send a multicast packet, a node will send _______.

   a. One packet to one of the rings

   b. One packet for every node on the ring

   c. One packet for each node it wants to receive it

   d. One packet on each ring

9. The bandwidth control algorithm will___________.

   a. Decide how much high-priority data a node can send

   b. Decide how much low-priority data a node can send

   c. Make sure the ring is using all the available bandwidth

   d. Decide who has the token to send traffic

10. Resilient packet rings are not applicable for _________.

   a. Metro networks (MANs)

   b. Intra–POP networks

   c. Cable MSO networks

   d. None of the above

# Correct Answers

1. Resilient packet rings are transported over a ________ topology.

   **a. Dual fiber**

   b. Dual copper

   c. Wireless

   d. Laser

2. Resilient packet rings carry multiple services except _________.

    a. Internet Data

    b. Voice over IP

    **c. Native TDM**

    d. Packetized TDM

3. Jitter- and latency-sensitive traffic uses the _______ of RPRs.

    a. Normal service

    b. Bandwidth-control information

    **c. High-priority service**

    d. Control information

4. The IEEE standard for RPRs is ________.

    a. 802.1

    b. 802.3

    c. 802.16

    **d. 802.17**

5. When using the same physical layer, RPR can be transported within existing _______ networks.

    **a. SONET/SDH**

    b. ATM

    c. Token-ring

    d. Ethernet

6. A RPR node finds the other nodes on the ring via ________.

   a. Operator provisioning

   **b. Automatic topology discovery**

   c. Master topology list distribution

   d. Broadcast

7. A single fault on a RPR ring will be protected within _______.

   a. 10 seconds

   b. 100 ms

   c. 50 us

   **d. 50 ms**

8. To send a multicast packet, a node will send _______.

   a. One packet to one of the rings

   **b. One packet for every node on the ring**

   c. One packet for each node it wants to receive it

   d. One packet on each ring

9. The bandwidth control algorithm will___________.

   a. Decide how much high-priority data a node can send

   **b. Decide how much low-priority data a node can send**

   c. Make sure the ring is using all the available bandwidth

   d. Decide who has the token to send traffic

10. Resilient packet rings are not applicable for _________.

   a. Metro networks (MANs)

   b. Intra–POP networks

c. Cable MSO networks

**d. None of the above**

# Glossary

## Acronyms Guide

**MPLS**
Multiprotocol Label Switching

**MSO**
Multiple-System Operator

**RPR**
Resilient Packet Ring

**SDH**
Synchronous Digital Hierarchy

**SONET**
Synchronous Optical Network

**TDM**
Time Division Multiplexing

**VPN**
Virtual Private Network

## Definitions

**CRC**
The Cyclic Redundancy Check is an error-checking technique that uses a calculated numeric value to detect errors in transmitted data.

**IEEE 802.17**
The IEEE working group working on an international standard for RPR.

**IETF**
Internet Engineering Task Force is responsible for developing Internet standards. The IETF operates under the auspices of the Internet Society (ISOC).

**MAC**
The Media Access Control is the Layer-2 function responsible for access to the medium (fiber, coax, etc.). Ethernet and RPR both have defined MAC layers.

**SRP**
Spatial Reuse Protocol, a Cisco Systems MAC–layer protocol currently published as Internet Engineering Task Force (IETF) RFC 2892.

**TTL**
Time To Live, a value decremented within a packet at each hop. TTL keeps packets from circulating indefinitely.