Ethernet Ring Protection Switching

White Paper

Omnitron Systems

ITU-T G.8032 Ethernet Ring Protection Switching

Evolution of Ring Protection Switching

Synchronous Optical Networking (SONET) and Synchronous Digital Hierarchy (SDH) were the predominant ring transport networks deployed by Service Providers. SONET/SDH networks provided Service Providers a reliable transport network with sub-50msec service protection.

With the introduction of Carrier Ethernet by the Metro Ethernet Forum (MEF), ring topologies using Ethernet networks were required to meet the protection objectives used by SONET/SDH. Utilizing Ethernet in a ring topology provides efficient network connectivity, supporting multiple services while allowing flexible deployment scenarios for Access, Metro and Core network applications. Traditionally, Ethernet networks used Spanning Tree Protocol to ensure a loop-free topology. However, switchover times were too long, and inconsistent.

The ITU-T defined a method to achieve the same protection used by SONET/SDH transport networks for Ethernet ring topologies. ITU-T G.8032 Ethernet Ring Protection Switching (ERPS) achieved this protection by having each ERPS node in the ring send messages to its neighboring node to determine its availability. When a fiber loss occurs, the failure is immediately determined and an alternate path is established. When used in conjunction with IEEE 802.1ag Connectivity Fault Management (CFM), a 3.3 millisecond messaging interval can be configured to ensure rapid service restoration.

ERPS Configuration Types

ERPS uses the G.8032 Ethernet Ring Protection (ERP) protocol to provide protection for Ethernet traffic on the ring. This protection ensures that no Ethernet data loops are created by the ring. Loops are prevented by blocking traffic on a predetermined link, called the Ring Protection Link (RPL). Links are essentially several point to point links, and treated as such with ERP. Nodes on the ring communicate using control messages called Ring Automatic Protection Switching (R-APS) messages. These messages communicate the status and configuration of the ring.

There are three types of ERPS configurations:

1. Port-based ERPS configurations provide protection to the ports on the ring and not individual Ethernet Virtual Circuits (EVCs). An Automatic Protection Switching (APS) EVC must still be configured in order to provide status and configuration messaging between the nodes. All data traffic will be switched over during a fault condition.
2. EVC-based ERPS configurations provide protection to individual EVCs. The EVC-based ERPS configuration allows multiple EVCs to be protected, depending on the critical nature of the data traffic on the ring. A separate APS EVC must be configured in order to provide status and configuration messaging between the nodes.
3. Configurations utilizing IEEE 802.1ag Connectivity Fault Management provide protection to individual EVCs and guaranty sub-50msec protection switching using 3.3msec Connectivity Check Messages (CCM). A separate APS EVC must be configured in order to provide status and configuration messaging between the nodes, functioning as point-to-point links monitored by 802.1ag.

These three configurations perform the same basic ring protection functions. 802.1ag based configurations have faster failover times for larger fiber rings due to the speed of Connectivity Check Messages.

Network Topologies

The network topologies in this section support all three configuration types described earlier and the rings can be dual fiber or single-fiber. An ERPS ring consists of at least two nodes to a maximum of 16 nodes.

In this four-node ERPS Ring (Figure 1), each node has a Network Interface Device (NID) that is connected to the ring via two ports called Ring Ports. An ERPS ring must have one Ring Protection Link (RPL), with a NID at each end of the RPL. One NID is configured as the RPL Owner and an adjacent node is configured as the RPL Neighbor. Two other NIDs are deployed as Ring Nodes.

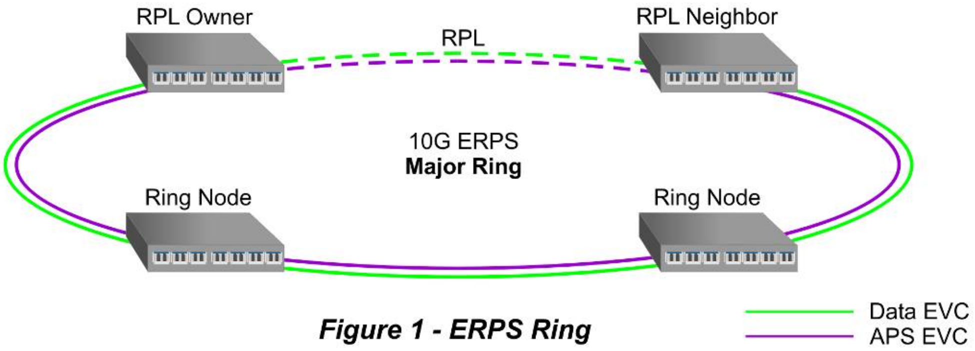


Figure 1 - ERPS Ring

At a minimum, two channels (or paths) are defined on the ring. One is the control channel or Automatic Protection Switching (APS) messaging channel, shown in purple, and one is the protected channel or data traffic, shown in green.

ERPS supports Sub Ring topologies. A Sub Ring is connected to the Major Ring at interconnecting NIDs. A Sub Ring has the option to be configured as a closed or open ring.

A Closed Sub Ring (Figure 2) shares a path on the Major Ring called a Virtual Channel. The Virtual Channel allows the APS messages of the Sub Ring to form a complete ring. Because the Virtual Channel forms a complete ring through the interconnecting Ring Nodes on the Major Ring, failure times are improved.

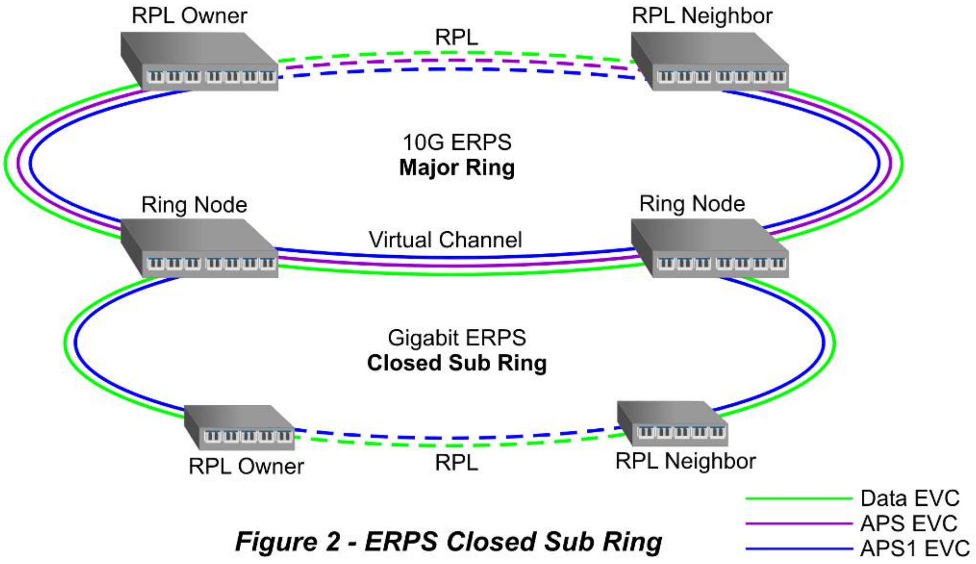


Figure 2 - ERPS Closed Sub Ring

An open Sub Ring (Figure 3) terminates the APS messages at each of the interconnecting Ring Node and does not use any resources on the Major Ring. The Sub Ring APS messages only travel over the RPL and associated links of the Sub Ring.

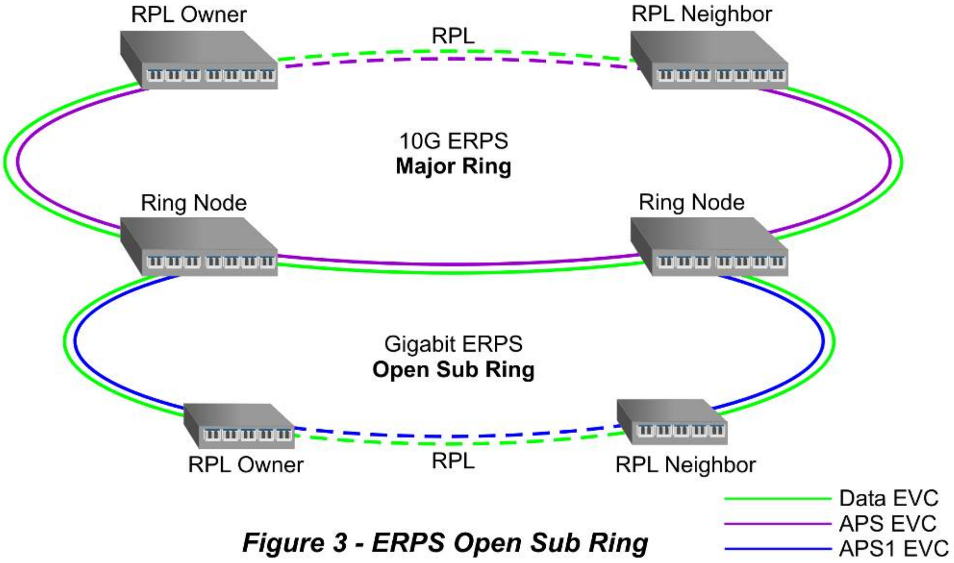


Figure 3 - ERPS Open Sub Ring

Open Rings are better suited for complex topologies with multiple rings. Closed Rings are better for topologies that are not as complex and require faster failover times.

How ERPS Works

The application diagrams in this section show three NIDs on an ERPS ring that are configured as the RPL Owner, RPL Neighbor and Ring Node. The RPL Owner controls the state of the ring. It is responsible for blocking and unblocking traffic on the RPL based on the state of the nodes on the ring.

This ring is configured as a port-based ERPS ring (Figure 4), and the iConverter NIDs use Automatic Protection Switching (APS) messages to monitor the ring. These messages are used to determine the state of the RPL (unblocked or blocked). Under normal conditions (no failures), the RPL Owner will block traffic on one end of the RPL and the RPL Neighbor will block the traffic at the other end.

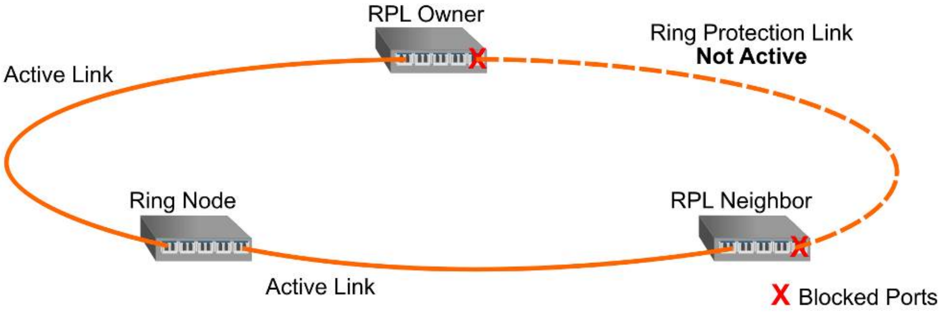


Figure 4 - ERPS Ring Normal State

When a failure on the ring occurs, the NIDs adjacent to the failed link will generate an APS signal failure message (APS alarm) to the RPL owner (Figure 5).

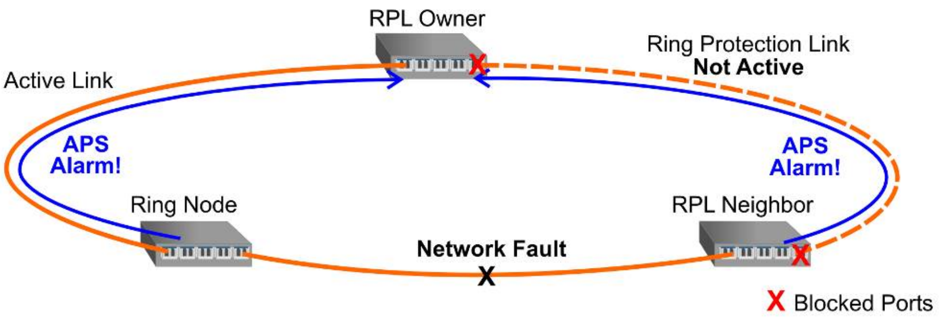


Figure 5 - Network Fault and APS Alarms

Once the RPL Owner receives the signal fail messages, the RPL Owner will unblock the RPL and send R-APS messages causing the RPL Neighbor to unblock the RPL, allowing the RPL to be used for data traffic (Figure 6). The RPL owner also blocks the ports on the NIDs at each end of the network fault.

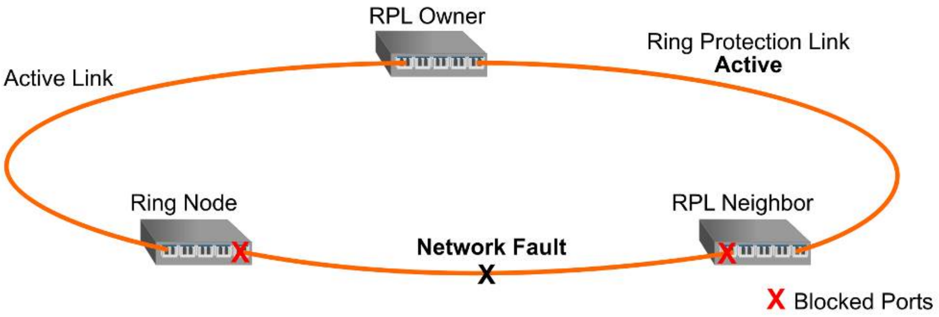


Figure 6 - Swithover to RPL Active

When a failed link is restored, the NIDs adjacent to the restored link will send APS restore, or clear signal fail messages (Figure 7).

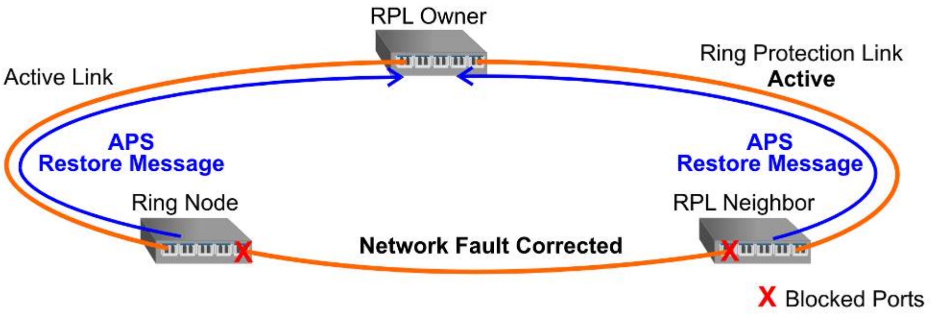


Figure 7 - Network Fault Corrected and Restore Messages

Upon receipt of the APS restore messages, the Ring Owner will block the RPL after the network has stabilized. The APS restore messages will cause the NIDs at each end of corrected fault link to unblock all blocked ports (Figure 8).

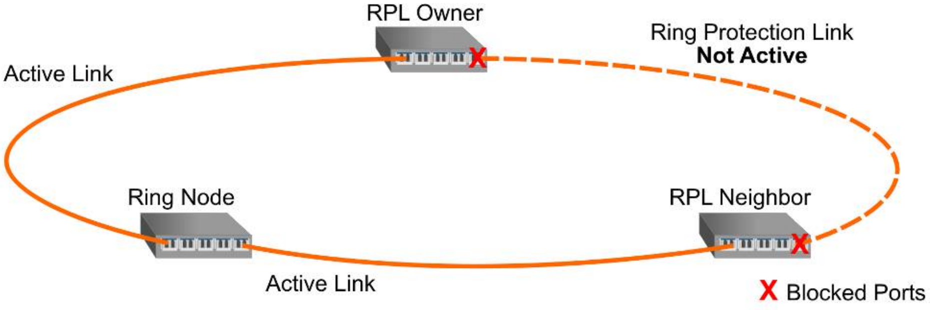
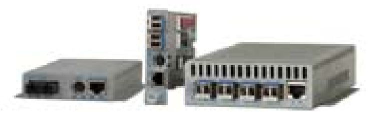


Figure 8 - ERPS Ring Returns to Normal State

Network Interface Devices

iConverter Carrier Ethernet 2.0 certified Network Interface Devices provide comprehensive support for the ITU-T G.8032 ERPS standard. iConverter NIDs support port-based, EVC-based and IEEE 802.1ag based configurations. IEEE 802.1ag CFM with fast Connectivity Check Messages (CCM) enables 3.3msec rate and sub-50msec protection switching for mobile backhaul and mission-critical business services. iConverter NIDs support for Main Ring and both open and closed Sub-Ring configurations.

iConverter GM4 Gigabit NIDs, GM4 PoE NIDs, XM5 10G NIDs, and XM5 Demarcation and Aggregation NIDs support the ITU-T G.8032 ERPS standard.



iConverter GM4 Gigabit NIDs

iConverter XM5 10G Demarcation and Aggregation NIDs

Utilizing both ITU and IEEE industry standards, iConverter NIDs allow Service Providers to implement a comprehensive solution that provides end-to-end fault detection, performance monitoring and protection of the entire network.

iConverter NIDs that support ITU-T G.8032 ERPS provide tangible benefits to service providers, mobile operators and cable MSOs:

- Increased revenue from SLA-assured protected services
- Lowered operating costs by reducing service calls
- Improved customer satisfaction with predictable reliability