Estándar RPR, nueva solución de transporte capa 2 sobre anillos MAN/WAN de FO basada en conmutación de paquetes

Raúl Gutiérrez García, MSc.
Universidad ISPJAE, Ciudad Habana, Marianao, Cuba, servipl@ceniai.inf.cu

Carmen Moliner Peña, Dra.
Universidad ISPJAE, Ciudad Habana, Marianao, Cuba, carmen@tesla.cujae.edu.cu

Resumen

El crecimiento del tráfico de datos en redes de mediano y largo alcance, producido fundamentalmente por aplicaciones y servicios que requieren un ancho de banda grande, está originando el agotamiento de las capacidades de las infraestructuras de redes que se encuentran desplegadas en estos escenarios, que están soportadas en su mayoría sobre tecnologías basadas en conmutación de circuitos y que hacen un uso ineficiente del ancho de banda global de estas redes.

En los entornos MAN y WAN la topología en anillos de fibra óptica es la más difundida utilizando SONET/SDH como tecnología de transporte, pero debido a los problemas que hemos mencionado, la migración hacia tecnologías basadas en paquetes como Ethernet y RPR (Resilient Packet Ring), se vislumbra como la mejor alternativa para multiplicar las capacidades de las actuales infraestructuras descongestionando las redes y permitiendo brindar nuevos servicios.

RPR es una tecnología emergente basada en conmutación de paquetes y diseñada para topologías en anillos de fibra óptica, que mantiene la eficiencia de Ethernet en el transporte de los datos así como las ventajas de SONET/SDH en cuanto a tolerancia a fallos, tiempos de recuperación menores a 50ms, gestión amplia de la comunicación, etc. Por otra parte RPR incorpora otros beneficios importantes como son: reuso del espacio y administración justa del ancho de banda, que le permiten alcanzar altos niveles de ocupación del ancho de banda global de la red.

Palabras Claves: RPR

Introducción

El acelerado crecimiento del tráfico de datos junto a las ineficiencias de las actuales redes de mediano y largo alcance, que mayoritariamente están basadas en tecnologías orientadas a circuitos como SONET/SDH, provocan hoy el agotamiento de las capacidades de estas infraestructuras de transporte. La solución para que los proveedores de servicio puedan asimilar mayor cantidad de tráfico o soportar nuevos servicios podría ser invertir para desplegar más equipamiento y fibra óptica que doten a la red de mayores capacidades o recursos, pero tecnologías como SONET/SDH y ATM tienen un precio en

equipamiento, instalación y mantenimiento muy elevado. Otra variante puede ser utilizar equipos WDM para multiplicar las capacidades de la infraestructura existente, pero la tecnología WDM es muy cara actualmente. Finalmente, la solución más viable sería utilizar tecnologías orientadas a paquetes que transportan más eficientemente los datos, permitiendo un mejor aprovechamiento del ancho de banda e inclusive ofertando una capacidad total de ancho de banda por encima de la que físicamente posee la red.

Actualmente, el comportamiento del tráfico de dato genera cuellos de botellas fundamentalmente en las redes metropolitanas donde la topología más frecuente suele ser la de los anillos de fibra óptica. Los anillos ópticos son medios compartidos y Ethernet ha ido evolucionando hacia topologías punto a punto, de manera que Resilient Packet Ring (RPR) es la tecnología emergente orientada a paquetes que se concibe para este entorno, combinando las ventajas de SONET/SDH obtenidas del medio con la alta eficiencia de Ethernet para transportar los datos.

Desarrollo

Limitaciones de SONET/SDH

Se deben fundamentalmente a que estas tecnologías fueron diseñadas para manejar tráfico TDM empleando conmutación por circuito.

Circuitos Fijos: Se proveen circuitos fijos y rígidos entre dos nodos del anillo con un ancho de banda constante que se desperdicia cuando no se utiliza este enlace.

Desperdicio de ancho de banda en topologías lógicas tipo malla: Cuando se necesita comunicar todos los nodos del anillo (topología totalmente mallada, ampliamente utilizada) se hace un uso extremadamente ineficiente del ancho de banda global del anillo.

Tráfico Multidifusión: Se establece un circuito por cada comunicación y se transmite innecesariamente varias copias del paquete que circularán por el anillo ocupando un ancho de banda superior al necesario.

Desaprovechamiento del ancho de banda de protección: En condiciones normales de trabajo (no ocurrencia de eventos de fallos) el 50 % del ancho de banda global no se utiliza, sino que es reservado para garantizar tolerancia a fallos con tiempos de recuperación menores a 50ms.

Limitaciones de Ethernet

Tolerancia a fallos ineficiente: Ethernet de forma inherente no implementa mecanismos para lograr tolerancia a fallos, en su lugar se complementa con el protocolo de árbol extendido para crear caminos alternativos y recuperarse de fallos en la topología. En anillos de fibras ópticas este protocolo sólo consigue tiempos de recuperación en el orden de los 500 ms, que en comparación con los 50 ms logrados por SONET/SDH, resulta totalmente inconveniente para escenarios MAN y esto se debe a que al ocurrir una falla se necesita comunicar en serie al resto de los nodos para reconfigurar trayectorias alternativas.

Administración injusta del ancho de banda global del anillo: Al usarse el protocolo de árbol extendido para lograr tolerancia a fallos, sólo se permite una trayectoria activa entre dos nodos y esto convierte al anillo en una topología virtual punto a punto, donde a nivel de nodo no se asigna equitativamente el ancho de banda global del anillo.

Beneficios de RPR

Eficiencia en el uso del ancho de banda: RPR posee varias características que le permiten administrar eficientemente el ancho de banda total. En este caso los dos anillos que conforman la topología son utilizados tanto para tráfico de trabajo como para control y no se reserva ancho de banda para protección, significa que el 100 % del ancho de banda se utiliza en condiciones de funcionamiento normal. Gracias al mecanismo de auto-descubrimiento de topología, el tráfico "Unicast" se envía por el anillo que tiene la distancia más corta al nodo destino. En RPR los paquetes "Unicast" se extraen del anillo en el nodo destino permitiendo reusar el espacio y multiplicar el ancho de banda, mientras que para los paquetes "Multidifusión" se emplea un mecanismo que permite de forma eficiente compartir esta información por el resto de los nodos destinos sin que circule más de una copia por el anillo. Con respecto a la repartición del ancho de banda global disponible, a cada nodo se le asigna una porción equivalente para ser utilizada por el tráfico de baja prioridad en virtud del algoritmo de justicia (SRP-fa) definido por el estándar.

Servicios: RPR posee diferentes clases de servicios que le permiten manejar flujos de requisitos y exigencias diferentes.

Fácil de administrar: RPR ofrece simplicidad de administración PnP gracias a los mecanismos de auto-descubrimiento de topología y auto-protección. Para hacer cambios en la estructura, como agregar o quitar un nodo, no se necesita prácticamente la intervención de personal técnico.

Tolerancia a fallos: Las redes RPR se protegen automáticamente contra cortes en las fibras e interrupciones en los nodos que conforman el anillo, recuperándose en un tiempo menor de 50 ms. Cada nodo tiene dos caminos alternativos para llegar a cualquier destino dentro del anillo. Se definen dos mecanismos para la recuperación: puente (Wrap) y reencaminado (Steer) de los paquetes en un nodo, pero todos los nodos del anillo deben implementar el mismo mecanismo de protección.

Operación del anillo RPR

Las redes RPR están formadas por un conjunto de hasta 64 nodos y dos anillos ópticos que son utilizados ambos para transmitir tanto tráfico de trabajo como tráfico de control. Los paquetes de control de un anillo son siempre transmitidos por el anillo contrario en condiciones normales de operación (ausencia de fallos).

Cada nodo posee una dirección MAC de nivel 2 que lo identifica en el anillo y puede tener la capacidad de manejar las tramas llamadas "jumbos frames".

Cuando el anillo RPR comienza a trabajar, se intercambian tramas de auto-descubrimiento a intervalos de tiempo regulares que le permiten a cada nodo crear un mapa topológico con la información de todos los nodos de la red (distancia en saltos, estado, capacidad de manejar tramas gigantes, etc)

Cuando un nodo va a enviar un paquete de datos a otro nodo, primero se selecciona inteligentemente el anillo óptimo para alcanzar el nodo destino. El nodo fuente envía un paquete de control ARP utilizando multidifusión que al ser recibido por el nodo destino, este chequea su mapa topológico para averiguar por cual anillo la distancia al nodo fuente es mínima y responder la solicitud ARP enviando su dirección MAC en un paquete de control que viaja por el anillo contrario al que debe utilizarse. Cuando el nodo fuente recibe la respuesta ARP, comienza la transmisión de los datos por el anillo contrario al que recibió la respuesta. Ahora los paquetes de datos viajan por el anillo de menor trayectoria hasta llegar al nodo destino que lo extrae del anillo definitivamente garantizando con esto ocupar el ancho de banda, sólo en el tramo utilizado y dejando el resto del anillo libre para otras comunicaciones "Reuso del Espacio".

Operación del nodo RPR

Una ventaja básica de RPR mostrada en la figura 1 **[1]**, es que los nodos pueden asumir que los paquetes que se envían, eventualmente llegarán a su destino con independencia del camino que tomen, significa que sólo tres operaciones son necesarias: inserción de paquetes aportados por el nodo, tránsito de los paquetes que deben continuar hacia otro destino y extracción de los paquetes que están dirigidos al nodo. Este modo de operación le permite a cada nodo reducir el trabajo individual que tiene que realizar para comunicarse con los otros nodos del anillo, a diferencia de topologías malladas donde se necesita tomar la decisión acerca del puerto por donde se reenviará el paquete.

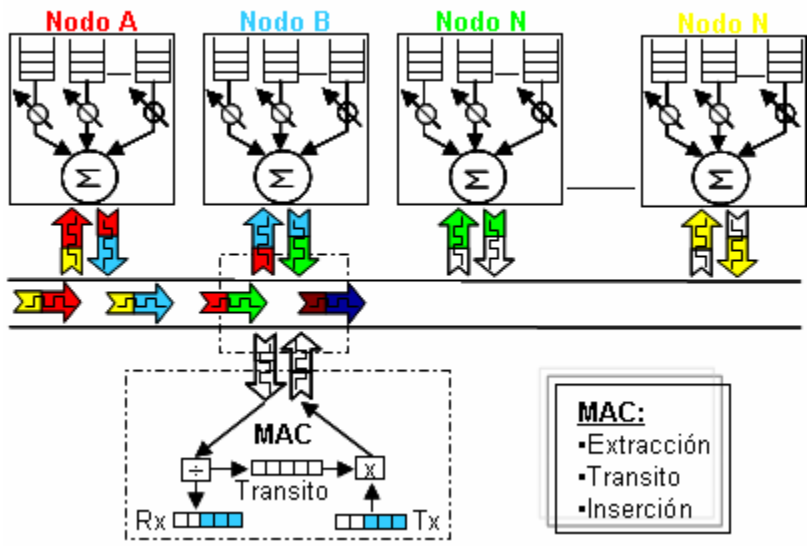

Figura 1. Operación del Nodo RPR. "Medio compartido"

Formato de la trama MAC

La capa MAC de IEEE 802.17 utiliza tres tipos de tramas:

1. Trama de datos. Trama que encapsula la PDU (Unidad de datos de protocolo) del cliente de la capa MAC
2. Trama de control (No incluye al algoritmo de justicia). Trama utilizada para administrar el anillo (funcionalidades de autodescubrimiento de topología, autorecuperación etc.)
3. Trama de control de justicia. Trama de negociación entre los nodos para la asignación justa del ancho de banda global del anillo.

Clases de servicio

RPR define tres clases de servicio para el tráfico que se maneja en el anillo:

1. ***Clase A:*** Tráfico de alta prioridad conforme al CIR reservado para esta clase. El tráfico clase A minimiza la latencia y las variaciones en la demora "jitter". Este tráfico no es afectado por el algoritmo de control de justicia o FCU. Existen dos variantes de esta clase: A0 que reserva el ancho de banda en el anillo (equivalente a un circuito en SONET/SDH) y que por tanto no puede utilizarse por otras comunicaciones y A1 que igualmente es tráfico de la más alta prioridad pero que permite disponer del ancho de banda que no esté utilizando, por otras comunicaciones.

2. ***Clase B:*** Tráfico de prioridad media conforme al CIR reservado para esta clase que no reserva ancho de banda. El tráfico contratado no es afectado por la FCU pero todo el tráfico que excede al CIR contratado se marca elegible para ser manejado por el algoritmo de justicia.
3. ***Clase C:*** Es una clase que se corresponde con la categoría "Mejor Esfuerzo" de IP. Todo el tráfico es marcado elegible para ser manejado por el algoritmo de justicia, que significa que saldrá al anillo con la menor prioridad y compartiendo con justicia el ancho de banda global del anillo no reservado, con el resto de los nodos que incorporan tráfico clase C al anillo.

Modelo de referencia de la capa MAC

La figura 2 muestra el camino que siguen los datos para ambos anillos **[2]** (transmisión, recepción y tránsito de la información) así como las funciones de control que se implementan por la capa MAC de RPR.

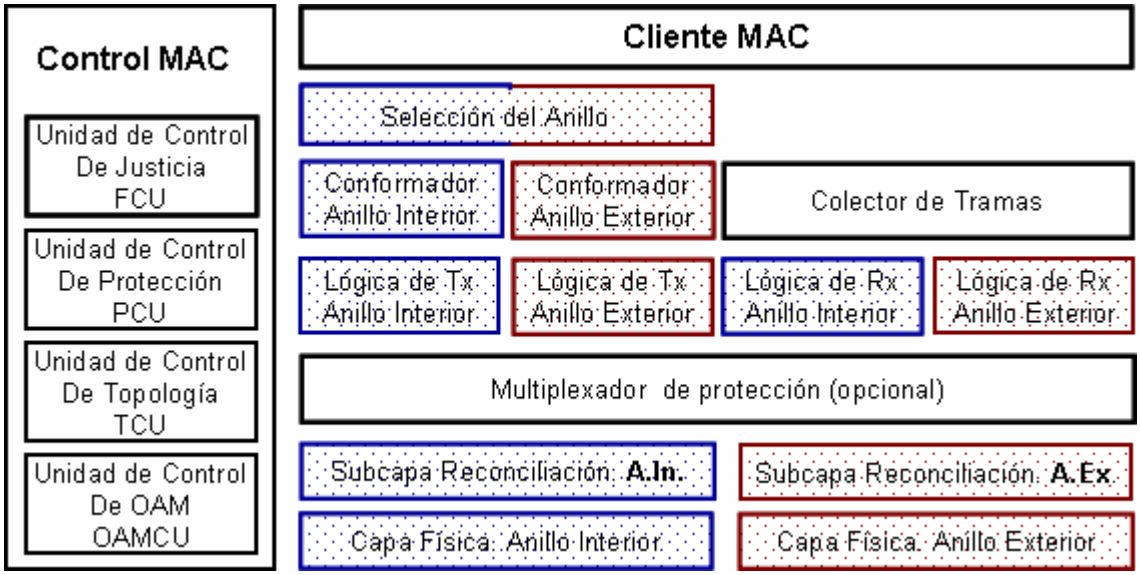

Figura 2. Modelo de referencia de la capa MAC IEEE 802.17

Recepción de los datos:
Los paquetes que llegan a la interfaz física de ambos anillos son traducidos a un formato consistente entendible por la subcapa MAC RPR y entregados a la lógica de recepción, en este bloque funcional se determina si el paquete va a ser procesado por el nodo y/o si continúa viaje por el anillo. Los paquetes "unicast" que tienen la dirección destino del nodo y los paquetes de difusión, son entregados al cliente MAC o a las unidades de control según corresponda y el resto de los paquetes pasan al buffer de tránsito para que sigan circulando por el anillo hacia su destino. El buffer de tránsito puede estar implementado con una o dos colas para tráficos de diferentes prioridades.

Transmisión de los datos:
La transmisión de los datos del cliente se realiza según los servicios contratados. Lo primero que se realiza es la selección del anillo a partir del mapa topológico que se crea mediante el proceso de auto-descubrimiento y con el mecanismo de resolución de direcciones ARP.

Durante eventos de protección en intervalos de fallas se puede redirigir el tráfico a este nivel para evitar los tramos que tienen dificultades. Posteriormente se le asigna un valor de tiempo de vida "TTL" al

paquete y se entrega al bloque conformador de tráfico responsable de regular la velocidad para los tráficos de cada clase de servicio, garantizando el ancho de banda contratado para las clases A y B así como ajustando la velocidad para el tráfico clase C y el excedente clase B según establezca el mecanismo de justicia. Este bloque conformador da permisos al cliente MAC para cada tipo de tráfico y anillo de forma independiente con el fin de evitar ráfagas y estabilizar el tráfico que entrega al bloque encargado de transmitir. La lógica de transmisión trabaja en función de la arquitectura de cola que implemente la capa MAC para el tráfico de tránsito y cumpliendo los siguientes principios:

- El tráfico local sale en orden de prioridad, primero la clase A, luego la clase B y finalmente la clase C.
- Buscar niveles máximos de utilización del ancho de banda
- Los paquetes que ya están en el anillo tienen que llegar a su destino
- El tráfico elegible para participar de la asignación justa del ancho de banda global disponible (no contratado por las clases A y B), comparte cuotas equivalentes de ancho de banda de justicia relativo al peso del nodo en cuestión.

Funciones de control de la capa MAC

Unidad de Control de Justicia (FCU)

La unidad de control de justicia "FCU" es la que garantiza a través del algoritmo de justicia "RPR-fa, que el ancho de banda del anillo elégible para ser compartido, sea asignado a los tráficos menos prioritarios (clase C y clase B que excede el CIR) compartiéndose de forma justa e inteligente entre todos los nodos que conforman el anillo. El algoritmo de justicia está diseñado de manera que favorece el reuso del espacio, significa que el ancho de banda en una sección del anillo se comparte por los nodos que utilizan esa sección, no ocupándose el recurso compartido en el resto del anillo. Por otra parte a cada nodo se le asigna un peso y esto permite que cada nodo tenga derecho a una asignación distinta en % del ancho de banda disponible para ser compartido por RPR-fa. **[3]**

La FCU tiene las siguientes características:

- Respuesta rápida
- Alta utilización del ancho de banda
- Escalabilidad
- Reclamo de ancho de banda
- Justicia basada en el peso de los nodos
- Soporte para clientes que procesan tramas de control de justicia de "Congestión-Múltiple"
- Estabilidad

La FCU tiene la función de enviar tramas de control de justicia que advierten al nodo que está arriba (del cual recibe las tramas de datos) la velocidad a que debe limitar el flujo elegible por RPR-fa, así mismo tiene la función de recibir estas tramas del nodo que está abajo y a través del conformador de tramas ajustar su velocidad permitida teniendo en cuenta el peso del nodo.

Unidad de Control de Protección (PCU)

IEEE 802.17 protege el tráfico contra fallos tanto en los nodos como en los diferentes tramos que conforman el anillo. Los mecanismos de protección permiten la inserción y extracción de nodos en el anillo sin necesidad de operaciones manuales. La información del estado del anillo se mantiene con el intercambio de paquetes de control entre los nodos en dos variantes, los nodos que detectan un evento de falla (nueva falla o restablecimiento) informan al resto, y periódicamente cada nodo transmite un paquete de control llamado "keepalive" que significa que el nodo esta funcionando correctamente. Se definen dos mecanismos para la recuperación: puente (Wrap) y reencaminado (Steer) de los paquetes en un nodo, pero todos los nodos del anillo deben implementar el mismo mecanismo de protección.

Características de la protección:

- Protección en un tiempo menor a 50ms tanto para tráfico "Unicast" como para tráfico de "Multidifusión".
- Soporte para ambos mecanismos de protección (puente y reencaminado de los paquetes)
- Soporte para la inserción y extracción dinámica de estaciones.
- No hay nodo master, cada estación opera independientemente.
- Escalabilidad a un número grande de estaciones.

Mecanismo de reencaminado de los paquetes:

Este mecanismo está programado por defecto ya que permite para el caso en que falle un tramo de fibra, obtener una disponibilidad mayor de ancho de banda que el mecanismo de puente. Al ocurrir un evento de protección todas las estaciones son notificadas sobre la localización de la falla, a partir de ese momento todas las estaciones que van a transmitir evitan el tramo con problema hasta que se reciba la notificación de restablecimiento. Un ejemplo de esta operación lo muestra la figura 3 **[4]**. Los paquetes que arriban al tramo que falla antes del tiempo de recuperación (menor a 50ms) se pierden. Los paquetes de "Multidifusión" son transmitidos por ambos anillos y el valor TTL se fija al número correcto de estaciones para cada anillo.

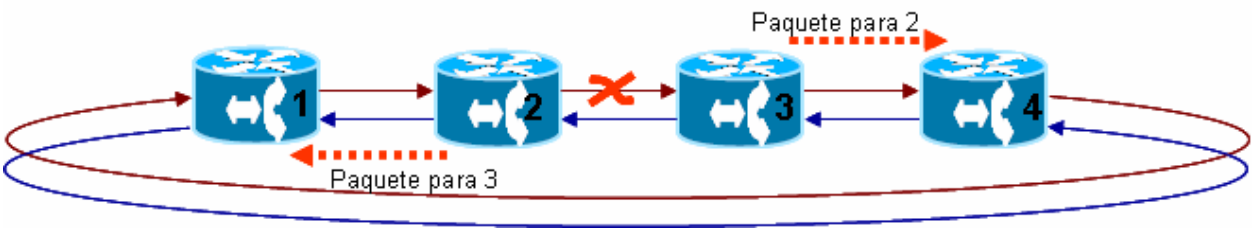

Figura 3. Mecanismo de reencaminado de los paquetes

Mecanismo de puente de los paquetes:

Este es un mecanismo opcional. Al ocurrir un evento de protección, los nodos adyacentes a la falla, puentean el tráfico que entra en la interfaz contraria a la falla hacía el otro anillo. Este evento de protección se notifica al resto de los nodos que eventualmente utilizarán el mecanismo de reencaminado de los paquetes si se encuentran lejos de la localización de la falla.

Jerarquía de protección:

Los mecanismos de protección tienen la capacidad de manejar diferentes fallas al mismo tiempo, estableciendo un orden de importancia que determina la atención que se brinda a éstas, significa por ejemplo que si existe una falla de "señal degradada" y se produce un evento que indica "falla de señal", se elimina la primera indicación de la base de datos y se reacciona en base a la segunda que es más importante. Este sistema permite conseguir una tolerancia a fallos más eficiente.

Estados de falla en orden decreciente de severidad:

- Conmutación forzada: Un operador inició un comando para forzar un evento de protección en una interfaz.
- Falla de señal: Una falla de señal correspondiente al medio físico o asociada al mensaje "keepalive" causa un evento de protección.
- Degradación de señal: Evento de protección producido por exceso de bits erróneos.
- Conmutación manual: Similar a conmutación forzada pero de menor prioridad.
- Retardo para la restauración de una falla: El tiempo de retardo configurable para restablecer un enlace después de haberse limpiado la falla.

Unidad de Control de Topología (TCU)
RPR define un mecanismo de descubrimiento de topología que permite crear y mantener en cada nodo una base de datos o mapa topológico que contiene la información de estado, capacidades y localización de todos los nodos RPR en el anillo doble de FO.

Los mensajes de control de topología son mensajes de difusión que se generan periódicamente o cuando un nodo detecta localmente un cambio de estado.

Características de la topología:
- Registro de conectividad de la estación y orden
- Rápida difusión de una imagen consistente a través del anillo
- Operación independiente de cada nodo sin necesidad de un nodo master
- Soporte para la inserción y extracción dinámica de estaciones

Operación del mecanismo de autodescubrimiento de topología:
- *Inicialización:* Al inicio el mapa topológico de un nodo solo tiene información local. Con el tiempo comienza a recibir los mensajes de difusión de otros nodos que le permiten crear su base de datos topológica de la red e igualmente comienza a difundir su información de topología periódicamente o al detectar cambios localmente.
- *Inserción de una estación nueva:* Cuando una estación se une al anillo, como parte de su inicialización envía un mensaje de difusión con su información topológica. El resto de los nodos al recibir el mensaje y detectar un cambio, lo reflejan en sus bases de datos y envían el mensaje de control de descubrimiento de topología con su información. De esta forma la nueva estación en breve puede actualizar su mapa topológico con la información de todos los nodos de la red RPR.
- *Falla:* Cuando una estación es extraída, falla, o se interrumpe un tramo, las estaciones adyacentes lo detectan y reflejan en su mapa topológico, luego se generan los mensajes de protección que permiten a cada nodo reflejar el cambio de conectividad y en consecuencia reencaminar el tráfico.

Unidad de Control de OAM (OAMCU)
Las funciones de OAM definidas por IEEE 802.17 ofrecen tres servicios de administración al cliente MAC: administración de configuración, administración de fallas y administración de rendimiento. Para la gestión se define una interfaz consistente a una MIB "Base de información de administración", que le permite a la entidad de administración obtener "GET" y/o fijar "SET" parámetros de configuración, topología y protección.

Se utilizan mensajes de eco/respuesta para monitoreo de conectividad y localización de camino entre nodos. Una trama de eco puede solicitar una respuesta con determinada clase de servicio, modo de protección, anillo, etc.

Interfaces físicas

IEEE 802.17 es un estándar de capa MAC que asimila en principio cualquier implementación de capa física. Sí es necesario definir una subcapa de reconciliación responsable de traducir las señales eléctricas de la interfaz física en particular al formato consistente de la interfaz común RPR MAC. El estándar define hasta el momento interfaces para la capa física de SONET/SDH y Ethernet.

Interfaz SDH/SONET
Se definen dos subcapas de reconciliación para SONET/SDH:

1. SRS “Subcapa de Reconciliación SONET/SDH”. Define una encapsulación similar al protocolo de enlace HDLC para tramas RPR con carga útil SONET/SDH similar a la encapsulación POS “Paquetes sobre SONET”
2. GRS “Subcapa de reconciliación GFP”. Define un mecanismo de encapsulación utilizando GFP “Protocolo de entramado genérico”

Interfaz Ethernet

Se definen dos subcapas de reconciliación para Ethernet:

1. GERS “Subcapa de Reconciliación Gigabit Ethernet”. Define una interfaz entre RPR MAC y la interfaz GMII.
2. XGERS “Subcapa de reconciliación 10 Gigabit Ethernet”. Define interfaces entre RPR MAC y las interfaces XGMII / XAUI.

Interfaces físicas Ethernet soportadas por IEEE 802.17:

- GbE PHY: 1000BASE-SX, 1000BASE-LX
- 10 GbE LAN PHY: 10GBASE-SR, 10GBASE-LR, 10GBASE-ER, 10GBASE-LX4
- 10 GbE WAN PHY: 10GBASE-SW, 10GBASE-LW, 10GBASE-EW

Alternativas de aplicación

La tecnología RPR hoy puede ser desplegada en tres escenarios (figura 4): **[5]**

1. Directamente sobre fibra óptica oscura, pudiéndose utilizar regeneradores para aumentar la distancia entre nodos. En este caso la interfaz física puede ser SONET/SDH o Ethernet
2. En infraestructuras WDM con nodos OADM “trasladadores de longitud de onda”
3. En infraestructuras SONET/SDH con nodos ADM “Multiplexor de adición/sustracción”

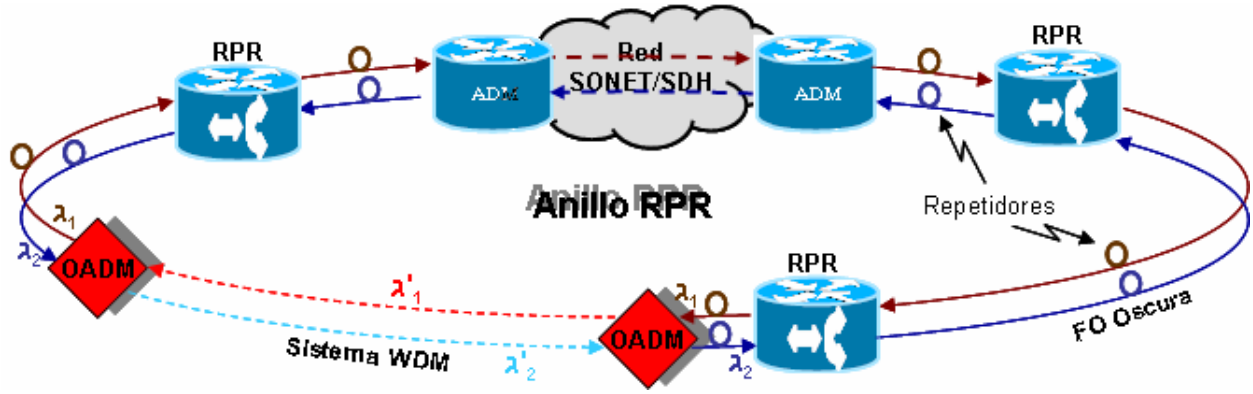

Figura 4. Conexión RPR a ADM, OADM(WDM) y FO Oscura

Conclusiones

RPR es una tecnología que ha sido diseñada sobre la base de la integración de las ventajas que poseen Ethernet y SONET/SDH, para capturar el mercado de las redes en anillo que se encuentran ampliamente difundidas, especialmente en entornos de área metropolitana.

Por una parte, IEEE 802.17 aprovecha la topología al igual que SONET/SDH para conseguir una tolerancia a fallos alta, con el empleo de dos mecanismos de recuperación automática y en tiempos

menores a 50ms, además permite una escalabilidad elevada con muy poca intervención de personal técnico, así como implementa una gestión amplia de operación, administración y mantenimiento, etc. Por otra parte al igual que Ethernet, logra un transporte muy eficiente de los datos, la transmisión entre dos nodos es asincrónica ocupándose justamente el ancho de banda necesario para transmitir los paquetes que se encuentren en las colas de tránsito y transmisión. Teniendo en cuenta además la naturaleza aleatoria y en ráfaga de los datos, es posible entonces asimilar los picos de velocidad que implica ofrecer un mejor servicio, etc.

RPR no se limita a copiar los beneficios de estas dos tecnologías sino que se incorporan una serie de funcionalidades adicionales. El algoritmo de justicia que permite administrar de una forma justa el ancho de banda del anillo, teniendo en cuenta además el peso de cada nodo, consigue niveles de ocupación del ancho de banda aun más elevados, adicionando oportunidades para el tráfico de menor prioridad. Con RPR se pueden manejar diferentes clases de tráficos, se brinda calidad de servicio e ingeniería de tráfico, ofreciéndose variados servicios de calidad para requerimientos y exigencias diferentes.

IEEE 802.17 es un estándar de capa MAC y no se ocupa de definir interfaces PMD, en su lugar define subcapas de reconciliación que permiten utilizar interfaces físicas basadas en estándares de otras tecnologías. Esto le permite a RPR una fácil, variada y rápida integración con las infraestructuras ya existentes.

Referencias

1. *Alianza RPR. (Octubre 2001). "An Introduction to Resilient Packet Ring Technology", http://www.rpralliance.org/articles/ACF16.pdf*
2. *Alianza RPR. (2003). "A summary and Overview of the IEEE 802.17 Resilient Packet Ring Standard, Draft version 2.0", http://www.rpralliance.org/articles/overview_of_draft_22.pdf*
3. *Alianza RPR. (Junio 2002). "Resilient Packed Ring, Fairness Protocol", http://rpralliance.org/articles/ACF1A.pdf*
4. *Ing. Raúl Gutiérrez García. (2004). "Soluciones para el empleo de redes Ethernet en escenarios MAN y WAN", Tesis de Maestría en Telemática 6ta Edición, Universidad ISPJAE, Ciudad Habana, Cuba.*
5. *Cisco System. (Julio 2002). "Spatial Reuse Protocol Technology", http://www.cisco.com/warp/public/cc/techno/wnty/dpty/tech/srpmc_wp.htm*
6. *Sitio Web del Grupo de tarea IEEE 802.17, URL: http://grouper.ieee.org/groups/802/17/*
7. *Sitio Web de la Alianza RPR, URL: http://www.RPRAlliance.org*

Información bibliográfica

MSc. Raúl GUTIÉRREZ GARCÍA. El ingeniero Raúl Gutiérrez García es graduado de la carrera de ingeniería en Telecomunicaciones del año 1991 y recién el pasado año terminó la maestría en Telemática. Actualmente ejerce como especialista en automática y colabora con la universidad cubana en proyectos de investigaciones relacionado con la rama de las telecomunicaciones. Ha participado como ponente en eventos internacionales desarrollados en su país, relacionados con la informática y las comunicaciones.

Dra. Carmen MOLINER PEÑA. La doctora en ciencias Carmen Moliner Peña es profesora titular de la universidad ISPJAE, trabaja e investiga en la rama de las comunicaciones, actualmente es la coordinadora de la Maestría en Telemática que se imparte en la universidad, tiene una participación activa en la preparación y como conferencista en todos los eventos nacionales e internacionales que se organizan en Cuba. Además imparte clases en universidades del extranjero, así como tutorea y opone tesis de la especialidad para los diferentes niveles, ingeniería, maestría y doctorado.

Glosario de términos

Término	Descripción
ADM	Multiplexor de adición y sustracción de flujos SONET/SDH "Add Drop Multiplexer"
ARP	Protocolo de resolución de direcciones IP -> MAC "Address Resolution Protocol"
ATM	Tecnología de transporte de datos "Modo de transmisión Asincrónico"(Asynchronous Transmission Mode)
CIR	Velocidad de tráfico convenida "Committed Information Rate"
FCU	Unidad de Control de Justicia de RPR "Fairness Control Unit"
FO	Fibra óptica
GMII	Interfaz independiente del medio de 1 GbE (Gigabit Media Independent Interface)
IEEE 802.17	Estándar RPR "Resilient Packet Ring" (en estado de borrador)
IP	Protocolo de Internet de la capa de red (Internet Protocol)
MAC	Subcapa de control de acceso al medio (Medium Access Control)
MAN	Red de área metropolitana (Metropolitan Area Network)
MDI	Interfaz dependiente del medio (Medium Dependent Interface)
MIB	Base de Información de Administración "Management Information Base"
OADM	Multiplexor óptico de adición y sustracción de flujos SONET/SDH "Optical Add Drop Multiplexer" "Transponder"
OAM	Operación, Administración y Mantenimiento "Operation, Administration and Maintenance"
PDU	Unidad de datos de protocolo "Protocol Data Unit"
PMD	Subcapa dependiente del medio (Physical Medium Dependent)
PnP	Tecnología de conecta y trabaja "Plug and Play"
RPR	Estándar IEEE 802.17 Resilient Packet Ring (en estado de borrador)
SDH	Jerarquía digital sincrónica (Synchronous digital hierarchy)
SONET	Red óptica sincrónica (Synchronous Optical Network)
SRP	Protocolo de reuso del espacio utilizado por la tecnología RPR "Spatial Reuse Protocol"
SRP-fa	Algoritmo de justicia del protocolo SRP "fairness algorithm"
TTL	Tiempo de vida de una trama o paquete "Time To Live"
WAN	Red de área amplia (Wide Area Network)
WDM	Multiplexación por división de longitud de ondas (Wavelength Division Multiplexing)
XGMII	Interfaz independiente del medio de 10 GbE (10 Gigabit Media Independent Interface)

Autorización

Los autores de este trabajo MSc. Raúl Gutiérrez García y Dra. Carmen Moliner Peña autorizan a LACCEI a publicar en las memorias del evento (CD y WEB) este documento.
Ni LACCEI ni los editores son responsables por el contenido de este documento y sus implicaciones.