Unión Internacional de Telecomunicaciones

# UIT-T

SECTOR DE NORMALIZACIÓN
DE LAS TELECOMUNICACIONES
DE LA UIT

# Y.2614

(08/2011)

SERIE Y: INFRAESTRUCTURA MUNDIAL DE LA INFORMACIÓN, ASPECTOS DEL PROTOCOLO INTERNET, REDES DE PRÓXIMA GENERACIÓN, INTERNET DE LAS COSAS Y CIUDADES INTELIGENTES

Redes de la próxima generación – Redes basadas en paquetes

## Fiabilidad de la red en las redes públicas de datos de telecomunicaciones por paquetes

Recomendación UIT-T Y.2614

Unión Internacional de Telecomunicaciones

RECOMENDACIONES UIT-T DE LA SERIE Y

**INFRAESTRUCTURA MUNDIAL DE LA INFORMACIÓN, ASPECTOS DEL PROTOCOLO INTERNET, REDES DE PRÓXIMA GENERACIÓN, INTERNET DE LAS COSAS Y CIUDADES INTELIGENTES**

| | |
|---|---|
| INFRAESTRUCTURA MUNDIAL DE LA INFORMACIÓN | |
| Generalidades | Y.100–Y.199 |
| Servicios, aplicaciones y programas intermedios | Y.200–Y.299 |
| Aspectos de red | Y.300–Y.399 |
| Interfaces y protocolos | Y.400–Y.499 |
| Numeración, direccionamiento y denominación | Y.500–Y.599 |
| Operaciones, administración y mantenimiento | Y.600–Y.699 |
| Seguridad | Y.700–Y.799 |
| Características | Y.800–Y.899 |
| ASPECTOS DEL PROTOCOLO INTERNET | |
| Generalidades | Y.1000–Y.1099 |
| Servicios y aplicaciones | Y.1100–Y.1199 |
| Arquitectura, acceso, capacidades de red y gestión de recursos | Y.1200–Y.1299 |
| Transporte | Y.1300–Y.1399 |
| Interfuncionamiento | Y.1400–Y.1499 |
| Calidad de servicio y características de red | Y.1500–Y.1599 |
| Señalización | Y.1600–Y.1699 |
| Operaciones, administración y mantenimiento | Y.1700–Y.1799 |
| Tasación | Y.1800–Y.1899 |
| Televisión IP sobre redes de próxima generación | Y.1900–Y.1999 |
| REDES DE LA PRÓXIMA GENERACIÓN | |
| Marcos y modelos arquitecturales funcionales | Y.2000–Y.2099 |
| Calidad de servicio y calidad de funcionamiento | Y.2100–Y.2199 |
| Aspectos relativos a los servicios: capacidades y arquitectura de servicios | Y.2200–Y.2249 |
| Aspectos relativos a los servicios: interoperabilidad de servicios y redes en las redes de la próxima generación | Y.2250–Y.2299 |
| Mejoras de las NGN | Y.2300–Y.2399 |
| Gestión de red | Y.2400–Y.2499 |
| Arquitecturas y protocolos de control de red | Y.2500–Y.2599 |
| **Redes basadas en paquetes** | **Y.2600–Y.2699** |
| Seguridad | Y.2700–Y.2799 |
| Movilidad generalizada | Y.2800–Y.2899 |
| Entorno abierto con calidad de operador | Y.2900–Y.2999 |
| REDES FUTURAS | Y.3000–Y.3499 |
| COMPUTACIÓN EN LA NUBE | Y.3500–Y.3999 |
| INTERNET DE LAS COSAS Y CIUDADES Y COMUNIDADES INTELIGENTES | |
| General | Y.4000–Y.4049 |
| Definiciones y terminologías | Y.4050–Y.4099 |
| Requisitos y casos de utilización | Y.4100–Y.4249 |
| Infraestructura, conectividad y redes | Y.4250–Y.4399 |
| Marcos, arquitecturas y protocolos | Y.4400–Y.4549 |
| Servicios, aplicaciones, computación y proceso de datos | Y.4550–Y.4699 |
| Gestión, control y calidad de funcionamiento | Y.4700–Y.4799 |
| Identificación y seguridad | Y.4800–Y.4899 |
| Examen y evaluación | Y.4900–Y.4999 |

*Para más información, véase la Lista de Recomendaciones del UIT-T.*

# Recomendación UIT-T Y.2614

## Fiabilidad de la red en las redes públicas de datos de telecomunicaciones por paquetes


### Resumen

En la Recomendación UIT-T Y.2614 se identifican los objetivos, la arquitectura y los mecanismos aplicables a la fiabilidad de la red en las redes públicas de datos de telecomunicaciones por paquetes (RPDTP), y se describen los mecanismos de protección de enlace, protección de camino, detección de fallos en la red, activación de la conmutación de protección y coordinación de la protección.



### Historia

| Edición | Recomendación | Aprobación | Comisión de Estudio | ID único* |
|---|---|---|---|---|
| 1.0 | UIT-T Y.2614 | 06-08-2011 | 13 | 11.1002/1000/11363 |

### Palabras clave

RFBP, protección de enlace, RPDTP, fiabilidad, protección de camino.


* Para acceder a la Recomendación, sírvase digitar el URL http://handle.itu.int/ en el campo de dirección del navegador, seguido por el identificador único de la Recomendación. Por ejemplo, http://handle.itu.int/11.1002/1000/11830-en.

## PREFACIO

La Unión Internacional de Telecomunicaciones (UIT) es el organismo especializado de las Naciones Unidas en el campo de las telecomunicaciones y de las tecnologías de la información y la comunicación. El Sector de Normalización de las Telecomunicaciones de la UIT (UIT-T) es un órgano permanente de la UIT. Este órgano estudia los aspectos técnicos, de explotación y tarifarios y publica Recomendaciones sobre los mismos, con miras a la normalización de las telecomunicaciones en el plano mundial.

La Asamblea Mundial de Normalización de las Telecomunicaciones (AMNT), que se celebra cada cuatro años, establece los temas que han de estudiar las Comisiones de Estudio del UIT-T, que a su vez producen Recomendaciones sobre dichos temas.

La aprobación de Recomendaciones por los Miembros del UIT-T es el objeto del procedimiento establecido en la Resolución 1 de la AMNT.

En ciertos sectores de la tecnología de la información que corresponden a la esfera de competencia del UIT-T, se preparan las normas necesarias en colaboración con la ISO y la CEI.

## NOTA

En esta Recomendación, la expresión "Administración" se utiliza para designar, en forma abreviada, tanto una administración de telecomunicaciones como una empresa de explotación reconocida de telecomunicaciones.

La observancia de esta Recomendación es voluntaria. Ahora bien, la Recomendación puede contener ciertas disposiciones obligatorias (para asegurar, por ejemplo, la aplicabilidad o la interoperabilidad), por lo que la observancia se consigue con el cumplimiento exacto y puntual de todas las disposiciones obligatorias. La obligatoriedad de un elemento preceptivo o requisito se expresa mediante las frases "tener que, haber de, hay que + infinitivo" o el verbo principal en tiempo futuro simple de mandato, en modo afirmativo o negativo. El hecho de que se utilice esta formulación no entraña que la observancia se imponga a ninguna de las partes.

## PROPIEDAD INTELECTUAL

La UIT señala a la atención la posibilidad de que la utilización o aplicación de la presente Recomendación suponga el empleo de un derecho de propiedad intelectual reivindicado. La UIT no adopta ninguna posición en cuanto a la demostración, validez o aplicabilidad de los derechos de propiedad intelectual reivindicados, ya sea por los miembros de la UIT o por terceros ajenos al proceso de elaboración de Recomendaciones.

En la fecha de aprobación de la presente Recomendación, la UIT no ha recibido notificación de propiedad intelectual, protegida por patente, que puede ser necesaria para aplicar esta Recomendación. Sin embargo, debe señalarse a los usuarios que puede que esta información no se encuentre totalmente actualizada al respecto, por lo que se les insta encarecidamente a consultar la base de datos sobre patentes de la TSB en la dirección http://www.itu.int/ITU-T/ipr/.

## ÍNDICE

## Introducción

La fiabilidad de la red en las redes públicas de datos de telecomunicaciones por paquetes (RPDTP) se garantiza a través de mecanismos de protección de enlace y de protección de camino. Ambos mecanismos comprenden dos tipos de protección, a saber, la protección 1:1 y la protección 1:n. En el marco del mecanismo de protección de caminos, es posible utilizar tres modelos de encaminamiento.

También cabe la posibilidad de utilizar tres modelos de encaminamiento – el modelo de encaminamiento por trayecto doble, el modelo de encaminamiento por trayecto más corto o el modelo de encaminamiento alternativo – a efectos de la protección de camino en las RPDTP.

– El modelo de encaminamiento por trayecto doble calcula previamente dos trayectos disociados conforme al método de descomposición en orejas, a fin de proporcionar una protección de tipo 1:1, desde el nodo de origen hasta el nodo de destino, de acuerdo con la topología de la red y la información de los recursos. Estos trayectos son el trayecto de servicio y el trayecto de protección.

– El modelo de encaminamiento por trayecto más corto y el modelo de encaminamiento alternativo pueden utilizarse conjuntamente para proporcionar una protección de tipo 1:n.

– Por sí solo, el modelo de encaminamiento alternativo puede proporcionar una protección de tipo 1:n y calcular varios trayectos, de los cuales uno funciona como trayecto de servicio y los demás como trayectos de protección.

# Recomendación UIT-T Y.2614

## Fiabilidad de la red en las redes públicas de datos de telecomunicaciones por paquetes

### 1 Alcance

En la presente Recomendación se identifican los objetivos, la arquitectura y los mecanismos aplicables a la fiabilidad de la red en las redes públicas de datos de telecomunicaciones por paquetes (RPDTP), y se describen los mecanismos de protección de enlace, protección de camino, detección de fallos en la red, activación de la conmutación de protección y coordinación de la protección.

### 2 Referencias

Las siguientes Recomendaciones del UIT-T y otras referencias contienen disposiciones que, mediante su referencia en este texto, constituyen disposiciones de la presente Recomendación. Al efectuar esta publicación, estaban en vigor las ediciones indicadas. Todas las Recomendaciones y otras referencias son objeto de revisiones por lo que se preconiza que los usuarios de esta Recomendación investiguen la posibilidad de aplicar las ediciones más recientes de las Recomendaciones y otras referencias citadas a continuación. Se publica periódicamente una lista de las Recomendaciones UIT-T actualmente vigentes. En esta Recomendación, la referencia a un documento, en tanto que autónomo, no le otorga el rango de una Recomendación.

[UIT-T Y.2601] Recomendación UIT-T Y.2601 (2006), *Características y requisitos fundamentales de las redes futuras basadas en paquetes*.

[UIT-T Y.2611] Recomendación UIT-T Y.2611 (2006), *Arquitectura general de las redes futuras basadas en paquetes*.

[UIT-T Y.2612] Recomendación UIT-T Y.2612 (2009), *Marco y requisitos genéricos del direccionamiento, encaminamiento y reenvío de la futura red de portador basada en paquetes*.

[UIT-T Y.2613] Recomendación UIT-T Y.2613 (2010), *Arquitectura técnica general para la red pública de paquetes de datos de telecomunicación*.

### 3 Términos y definiciones

#### 3.1 Términos definidos en otros textos

En la presente Recomendación se utilizan los siguientes términos definidos en otros textos:

**3.1.1 conmutación de protección bidireccional** [b-UIT-T I.630]: arquitectura de conmutación de protección en la que, en caso de fallo unidireccional, ambos sentidos, es decir, el sentido afectado y el sentido no afectado (del "camino", de la "conexión de subred", etc.), se conmutan a protección.

**3.1.2 tiempo de espera** [b-UIT-T G.870]: tiempo entre el aviso de señal degradada o de señal con fallo, y la activación del algoritmo de conmutación de protección.

**3.1.3 protección manual** [b-UIT-T M.2102]: la recuperación se inicia por conmutación forzada o manual al camino de alternativa; el retorno a la configuración original se efectúa por medio de conmutación forzada o manual al estado normal.

**3.1.4 funcionamiento no reversivo (protección)** [b-UIT-T G.870]: funcionamiento de conmutación de protección, en el que el transporte y la selección de la señal de tráfico normal no regresan a la entidad de transporte de servicio cuando terminan las peticiones de conmutación.

**3.1.5 conmutación de protección** [b-UIT-T I.630]: técnica de supervivencia de red con política de atribución de recursos de protección especializada.

**3.1.6 red pública de datos de telecomunicaciones por paquetes (RPDTP)** [UIT-T Y.2613]: red de datos por paquetes diseñada para el estrato de transporte de las NGN, que debe ser segura, fiable, controlable y gestionable y que puede cumplir todos los requisitos descritos en [UIT-T Y.2601]. La RPDTP es una red jerárquica, que puede subdividirse en varias capas de red.

**3.1.7 funcionamiento reversivo (protección)** [b-UIT-T G.870]: funcionamiento de conmutación de protección, en el que el transporte y la selección de la señal de tráfico normal (servicio) regresa siempre a (o permanece en) la entidad de transporte de servicio si terminan las peticiones de conmutación; es decir, cuando la entidad de transporte de servicio se ha recuperado del defecto o se despeja la petición externa.

**3.1.8 periodo de tiempo de conmutación** [b-UIT-T G.870]: periodo de tiempo entre el inicio del algoritmo de conmutación de protección y el momento en que se selecciona el tráfico de la entidad de transporte en reserva.

**3.1.9 protección de camino** [b-UIT-T G.780]: el tráfico normal se transporta/selecciona por un camino de protección en vez de por camino de servicio en caso de que este falle o si su calidad de funcionamiento cae por debajo de un nivel requerido.

**3.1.10 conmutación de protección unidireccional** [b-UIT-T I.630]: arquitectura de conmutación de protección en la que, en caso de un fallo unidireccional (es decir, un fallo que afecta solamente un sentido de la transmisión), se conmuta a protección sólo el sentido afectado (del "camino", de la "conexión de subred", etc.).

## 3.2 Términos definidos en la presente Recomendación

En la presente Recomendación se definen los siguientes términos:

**3.2.1 protección 1:1**: mecanismo de protección que envía el tráfico únicamente por el trayecto de servicio o por el trayecto de protección.

**3.2.2 modelo de encaminamiento alternativo**: modelo de encaminamiento que facilita múltiples trayectos entre un nodo de red pública de datos de telecomunicaciones por paquetes (RPDTP) de origen y un nodo RPDTP de destino.

NOTA – No es necesario que estos trayectos sean deterministas y únicos. En el marco de este modelo, el trayecto de emisión y el trayecto de recepción no se componen necesariamente de los mismos nodos y enlaces.

**3.2.3 modelo de encaminamiento por trayecto doble**: modelo de encaminamiento que facilita dos trayectos totalmente disociados entre un nodo de red pública de datos de telecomunicaciones por paquetes (RPDTP) de origen y un nodo RPDTP de destino.

NOTA – Estos trayectos pueden no ser los más cortos.

**3.2.4 protección de enlace**: mecanismo de protección de punto a punto.

NOTA – No conviene iniciar la conmutación de protección ni el reencaminamiento en la capa de red a menos que la protección de enlace falle.

**3.2.5 modelo de encaminamiento por trayecto más corto**: modelo de encaminamiento que facilita un trayecto determinista y único, que es el trayecto más corto entre un nodo de red pública de datos de telecomunicaciones por paquetes (RPDTP) de origen y un nodo RPDTP de destino.

NOTA – En el marco de este modelo, el trayecto desde el nodo de origen hasta el nodo de destino es el mismo que desde el nodo de destino hasta el nodo de origen.

## 4 Abreviaturas y acrónimos

En la presente Recomendación se utilizan las siguientes abreviaturas y acrónimos:

IP Protocolo Internet (*Internet protocol*)

JDS Jerarquía digital síncrona

MDLO Multiplexación por división de longitud de onda

OAM Operaciones, administración y mantenimiento

QoS Calidad de servicio (*quality of service*)

RPDTP Red pública de datos de telecomunicaciones por paquetes

## 5 Objetivos de fiabilidad de la red

En este apartado se describen los objetivos de fiabilidad de la red de una RPDTP.

### 5.1 Tiempo de conmutación

En función de los modelos de encaminamiento que soporte la RPDTP, el tráfico de servicio puede conmutarse del trayecto de servicio a un trayecto de protección en caso de fallo de un enlace o un nodo. El tiempo de conmutación se divide en dos: el tiempo que tarda el nodo en recibir el mensaje de notificación de fallo en la red enviado por el nodo más cercano al punto de fallo y el tiempo que tarda en completarse la conmutación de protección del trayecto de servicio al trayecto de protección.

En una RPDTP, el tiempo de conmutación no debería superar los 50 ms.

### 5.2 Tiempo de espera

Una RPDTP es una red de capas, cada una de las cuales comprende un mecanismo de protección. Por tanto, debe tenerse en cuenta la coordinación de la protección entre las capas, a fin de evitar conmutaciones de protección en un sentido y en otro. El tiempo de espera es útil en caso de interfuncionamiento de los mecanismos de protección. Cuando se declara una condición de defecto se inicia un temporizador de espera, cuya duración puede configurarse. Cuando el temporizador expira, la conmutación de protección se inicia si la condición de defecto sigue estando presente en el punto en cuestión. Cabe señalar que no es necesario que la condición de defecto esté presente durante todo el tiempo de espera; sólo importa el estado al expirar el temporizador de espera.

En una RPDTP, el tiempo de espera debería ser más largo que el de conmutación de la capa de red inferior.

### 5.3 Tipos de protección

Existen dos tipos de protección, a saber, la protección 1:1 y la protección 1:n. El tráfico de servicio puede transmitirse por el trayecto de servicio o por el trayecto de protección. El tipo de protección 1:1 prevé dos trayectos disociados entre el nodo de origen y el nodo de destino, siendo uno de ellos el trayecto de servicio y el otro el trayecto de protección. El tipo de protección 1:n prevé 1+*n* trayectos entre el nodo de origen y el nodo destino, siendo uno de ellos el trayecto de servicio y los *n* trayectos restantes los de protección.

En una RPDTP, se recomiendan los tipos de protección 1:1 y 1:n para la protección de camino.

### 5.4 Tipos de conmutación

Existen dos tipos de conmutación, a saber, la conmutación unidireccional y la conmutación bidireccional. En la conmutación unidireccional, los trayectos de emisión y recepción del tráfico son diferentes y, en consecuencia, sólo se conmuta el trayecto afectado. En la conmutación bidireccional,

los trayectos de emisión y recepción del tráfico suelen ser los mismos, por lo que ambos trayectos pueden conmutarse.

En una RPDTP, se recomienda proporcionar ambos tipos de conmutación, es decir, la unidireccional y la bidireccional.

### 5.5 Tipos de funcionamiento

Existen dos tipos de funcionamiento de protección, a saber, el funcionamiento irreversible y el funcionamiento reversible. Si se aplica el tipo irreversible, el servicio no vuelve al trayecto de servicio cuando este se recupera. El servicio sólo vuelve al trayecto de servicio en los casos en que falla el trayecto de protección actual. Si se aplica el tipo reversible, el servicio siempre vuelve al trayecto de servicio cuando este se recupera.

En una RPDTP, deben proporcionarse ambos tipos de funcionamiento, es decir, el reversible y el irreversible.

### 5.6 Protección manual

Una RPDTP soporta tanto la conmutación de protección automática, como la conmutación de protección manual. El operador puede efectuar la conmutación de protección manual, la cual suele ser prioritaria con respecto a la conmutación de la protección automática.

### 5.7 Criterios de iniciación de la conmutación

Una RPDTP soporta los siguientes criterios de iniciación de la conmutación:

- se inician instrucciones desde el exterior (por ejemplo, en caso de control manual);
- se produce un fallo de enlace o nodo en el trayecto de servicio, el trayecto de protección está preparado y el temporizador de espera ha expirado;
- se recupera el trayecto de servicio en el tipo de funcionamiento reversible.

## 6 Arquitectura de fiabilidad de la red

En una RPDTP, la protección de enlace y la protección de camino son necesarias conforme a lo siguiente:

- deben proporcionarse los tipos de protección 1:1 y 1:n;
- deben soportarse los tipos de conmutación unidireccional y bidireccional; y
- deben soportarse los tipos de funcionamiento reversible e irreversible.

### 6.1 Protección de enlace

Una RPDTP comprende numerosas capas y, en cada una de ellas, se prevé un mecanismo de protección. La protección de enlace funciona en la capa de enlace y es un mecanismo de protección de punto a punto. La conmutación de protección y el reencaminamiento no deben iniciarse en la capa de red a menos que la protección de enlace falle.

La Figura 6-1 ilustra la arquitectura de protección de enlace.

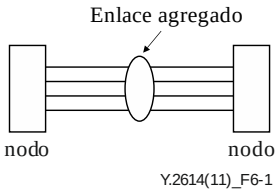


**Figura 6-1 – Arquitectura de protección de enlace**

En una RPDTP, existen dos mecanismos para la distribución del tráfico de servicio en los enlaces agregados:

1) El tráfico se distribuye en todos los enlaces físicos agregados, no obstante, conviene reservar parte de la capacidad de cada enlace, que se suma a la capacidad de uno o más enlaces, para garantizar la protección en caso de fallo de uno o más enlaces.

2) Uno o más enlaces agregados no transfieren tráfico a menos que uno o más enlaces agregados fallen.

Los nodos de extremo de los enlaces agregados pueden detectar fallos en uno o más enlaces físicos determinados y distribuir el tráfico del o los enlaces fallidos hacia otros enlaces físicos.

## 6.2 Protección de camino

La protección de camino es un mecanismo de protección de extremo a extremo. Conviene calcular previamente al menos dos trayectos desde el nodo de origen al mismo nodo de destino, de acuerdo con la topología de la red y la información de los recursos de la RPDTP. De estos trayectos, uno es el de servicio y el o los otros son los de protección.

Diversos paquetes sonda consecutivos se utilizan para detectar defectos en el trayecto de servicio o en el trayecto de protección. Cuando se recibe un mensaje de notificación de fallo en la red, el tráfico de servicio debe conmutarse del trayecto de servicio al de protección en el momento en que expira el temporizador de espera.

La Figura 6-1 ilustra la arquitectura de protección de camino.

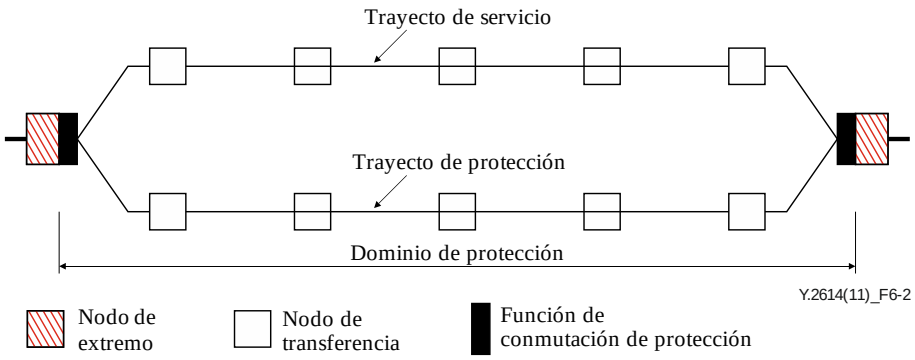


**Figura 6-2 – Arquitectura de protección de camino**

En una RPDTP, conviene proporcionar los tipos de protección 1:1 y 1:n para la protección de camino.

El tipo de protección 1:1 prevé la aplicación del modelo de encaminamiento por trayecto doble, que calcula previamente dos trayectos disociados conforme al método de descomposición en orejas.

El tipo de protección 1:n comprende dos métodos de aplicación:

1) El modelo de encaminamiento por trayecto más corto y el modelo de encaminamiento alternativo se utilizan conjuntamente. El modelo de encaminamiento por trayecto más corto proporciona un trayecto de servicio y el modelo de encaminamiento alternativo proporciona *n* trayectos de protección.

2) El modelo de encaminamiento alternativo se utiliza para calcular varios trayectos, siendo uno de ellos el trayecto de servicio y los demás los trayectos de protección.

Diversos paquetes sonda consecutivos se utilizan para detectar defectos en el trayecto de servicio o en el trayecto de protección. Estos se insertan en el extremo de origen del camino de protección y se detectan y extraen en el extremo de destino del camino de protección.

### 6.3 Tipos de conmutación

La conmutación de protección puede ser de tipo unidireccional o bidireccional.

En una RPDTP, los trayectos de emisión y de recepción suelen ser los mismos, si el trayecto se calcula conforme al modelo de encaminamiento por trayecto más corto o al modelo de encaminamiento por trayecto doble. En ambos casos, se aplica la conmutación bidireccional. Sin embargo, los trayectos de emisión y de recepción pueden ser diferentes si el trayecto se calcula conforme al modelo de encaminamiento alternativo. En ese caso, se aplica la conmutación unidireccional.

### 6.4 Tipos de funcionamiento

El funcionamiento de protección puede ser de tipo reversible o irreversible.

Si se aplica el tipo irreversible, tras la conmutación de protección del trayecto de servicio al trayecto de protección, el tráfico de servicio no vuelve al trayecto de servicio cuando este se recupera. El servicio sólo vuelve al trayecto de servicio en los casos en que falla el trayecto de protección actual y el trayecto de servicio se recupera.

Si se aplica el tipo reversible, el servicio siempre vuelve al trayecto de servicio cuando este se recupera. En una RPDTP, se recomienda el tipo de funcionamiento reversible.

### 6.5 Mecanismo de detección de fallos en la red

En una RPDTP existen dos mecanismos de detección de fallos en la red. El primero es el mecanismo de detección de fallos de enlace. Este funciona en la capa de enlace y detecta en tiempo real el estado de un enlace mediante la transmisión periódica de tramas de mantenimiento de enlace. El segundo es el mecanismo de detección de fallos de camino. Este funciona en la capa de red y detecta en tiempo real la conectividad de extremo a extremo mediante la transmisión periódica de paquetes OAM.

### 6.6 Mecanismo de activación de la conmutación de protección

La conmutación de protección debe activarse en los casos en que:

1) el operador la inicia (véanse la conmutación manual y la conmutación forzada) sin estar en curso una petición de conmutación con una prioridad más alta;
2) se declara un fallo de señal en el trayecto de servicio, pero no en el trayecto de protección, y el temporizador de espera ha expirado; o
3) expira el temporizador de espera de restablecimiento (modo reversible) y no se declara ningún fallo de señal en el trayecto de servicio.

## 7 Protección de enlace

En una RPDTP, dos nodos pueden conectarse a través de múltiples enlaces físicos para mejorar el ancho de banda y la fiabilidad entre ellos. Los diferentes enlaces físicos deben agregarse como un único enlace lógico al calcular la ruta, y el tráfico de servicio debe repartirse entre estos enlaces físicos múltiples de acuerdo con el ancho de banda de enlace. En caso de fallo de uno o varios de los enlaces de agregación, el tráfico de servicio transportado por el o los enlaces fallidos debe transferirse a otros enlaces disponibles, sin conmutarse del trayecto de servicio al de protección a menos que la protección de enlace falle.

En una RPDTP, los fallos de la protección de enlace se producen cuando:

1) todos los enlaces físicos agregados fallan;
2) uno o varios enlaces agregados fallan y la capacidad de los enlaces restantes no puede satisfacer las necesidades de tráfico.

Cuando la protección de enlace falla, se aplica un mecanismo de protección de camino.

## 8 Protección de camino

A efectos de la protección de camino en una RPDTP, se utilizan tres modelos de encaminamiento, a saber, el modelo de encaminamiento por trayecto doble, el modelo de encaminamiento por trayecto más corto y el modelo de encaminamiento alternativo.

En el modo sin conexión, un nodo RPDTP determina el modelo de encaminamiento con arreglo al valor del campo de protección, que se compone de dos bits situados en el encabezamiento de paquete [UIT-T Y.2613]. En caso de fallo (de enlace o nodo) en la red, o de recuperación del trayecto de servicio, el valor del campo de protección debe modificarse.

Si el valor del campo de protección es "00", debe aplicarse el modelo de encaminamiento por trayecto más corto. En ese caso, el tráfico de servicio puede verse interrumpido en caso de fallo (de enlace o nodo) en la red, a menos que se aplique el modelo de encaminamiento alternativo, en cuyo caso el valor del campo de protección debe reajustarse de "00" a "10". El modelo de encaminamiento alternativo permite garantizar la accesibilidad de la red, pero no la calidad de servicio.

Si el valor del campo de protección es "11" o "01", debe aplicarse el modelo de encaminamiento por trayecto doble. En ese caso, el tráfico de servicio puede conmutarse del trayecto de servicio al de protección en caso de fallo (enlace o nodo) en la red, o del trayecto de protección al de servicio en caso de recuperación del trayecto de servicio en modo de funcionamiento reversible. En consecuencia, el valor debe reajustarse de "11" a "01" o de "01" a "11". Cabe tener en cuenta que la calidad de servicio sólo puede garantizarse si los recursos de red son exactamente los mismos en el trayecto de servicio y en el trayecto de protección.

### 8.1 Modelo de encaminamiento por trayecto doble

El modelo de encaminamiento por trayecto doble calcula previamente dos trayectos disociados desde el nodo de origen hasta el nodo de destino en función de la topología de la red y de la información de los recursos. Dichos trayectos son el trayecto de servicio y el trayecto de protección. Además del nodo de origen y el nodo destino, existen otros enlaces o nodos comunes a los trayectos de servicio y de protección.

En el marco del modelo de encaminamiento por trayecto doble, la topología de red debe cumplir dos condiciones:

1) todos los nodos de la RPDTP deben estar conectados como mínimo a otros dos nodos;
2) todos los enlaces de la RPDTP deben ser bidireccionales.

El método de descomposición en orejas permite obtener dos diagramas orientados completamente distintos (véase la Figura 8-1).

El Apéndice I contiene más información sobre el método de descomposición en orejas.

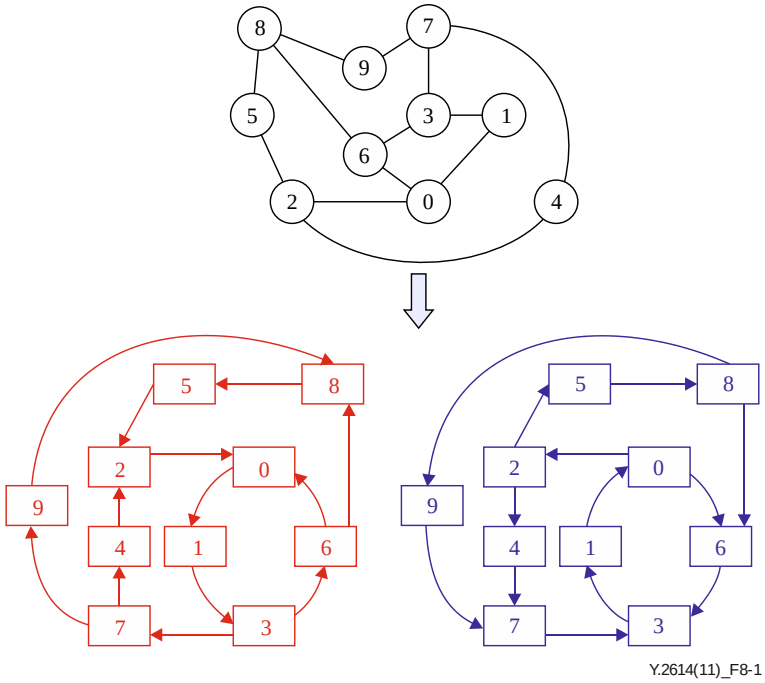


**Figura 8-1 – Descomposición en orejas en el modelo de encaminamiento por trayecto doble**

Según se indica en la Figura 8-1, entre dos nodos cualesquiera existen siempre dos trayectos disociados. Por ejemplo, del nodo 1 al nodo 7, se observa un trayecto de servicio que pasa por los nodos 1, 3 y 7 y un trayecto de protección que pasa por los nodos 1, 0, 2, 4 y 7.

En caso de fallo del trayecto de servicio, el nodo más cercano al punto de fallo envía un mensaje de notificación de fallo en la red al nodo de origen. Al recibir el mensaje de notificación, el nodo de origen conmuta el tráfico del trayecto de servicio al de protección. En ese caso, el valor del campo de protección del encabezamiento de paquete debe reajustarse de "11" a "01".

Si se aplica el tipo de funcionamiento reversible y el trayecto de servicio se recupera, el tráfico de servicio vuelve a conmutarse al trayecto de servicio. En este caso, el valor del campo de protección del encabezamiento de paquete debe reajustarse de "01" a "11".

Si se aplica el tipo de funcionamiento irreversible, aunque se recupere el trayecto de servicio, el tráfico de servicio no vuelve a conmutarse a dicho trayecto a menos que el trayecto de protección falle.

El modelo de encaminamiento por trayecto doble permite garantizar la calidad de servicio en caso de conmutación del trayecto de servicio al de protección, o viceversa, si los recursos de red son los mismos en ambos trayectos.

## 8.2 Modelo de encaminamiento por trayecto más corto

El modelo de encaminamiento por trayecto más corto facilita un trayecto determinista y único, que es el trayecto más corto desde el nodo RPDTP de origen hasta el nodo RPDTP de destino. En el marco de este modelo, los trayectos de emisión y de recepción deben ser los mismos. Cuando existen varias conexiones entre dominios RPDTP en el límite de dominio, la conexión con el mayor grado de prioridad es la única activa.

El valor del campo de protección del encabezamiento de paquete debe fijarse a "00" cuando se transmite un paquete utilizando el modelo de encaminamiento por trayecto más corto.

El modelo de encaminamiento alternativo se utilizará para garantizar la accesibilidad de la red en caso de fallo del modelo de encaminamiento por trayecto más corto. En ese contexto, el valor del campo de protección del encabezamiento de paquete debe reajustarse de "00" a "10".

### 8.3 Modelo de encaminamiento alternativo

En el marco del modelo de encaminamiento alternativo, numerosos trayectos se calculan previamente y se guardan en un cuadro de encaminamiento, siendo uno de ellos el trayecto de servicio. En caso de fallo del trayecto de servicio, se activa el segundo trayecto del cuadro de encaminamiento. Estos trayectos pueden no ser los más cortos, y los trayectos de emisión y de recepción no se componen necesariamente de los mismos nodos y enlaces. El modelo de encaminamiento alternativo puede utilizarse en dos casos:

1) El trayecto de servicio es el más corto; el modelo de encaminamiento alternativo proporciona uno o varios trayectos de protección.

   Un fallo en un nodo o un enlace o diversos cambios topológicos pueden provocar un fallo en el trayecto de servicio. En ese contexto, el modelo de encaminamiento alternativo facilita uno o varios trayectos de protección. En este caso, el valor del campo de protección del encabezamiento de paquete debe reajustarse de "01" a "00".

2) El modelo de encaminamiento alternativo proporciona tanto el trayecto de servicio como el o los trayectos de protección.

   En el marco del modelo de encaminamiento alternativo, el valor del campo de protección del encabezamiento de paquete debe fijarse en "01". Numerosos trayectos desde el nodo de origen hasta el nodo de destino se calculan previamente y se guardan en un cuadro de encaminamiento, y uno de ellos se utiliza como trayecto de servicio. En caso de fallo del trayecto de servicio, el trayecto de protección se elige entre los demás trayectos del cuadro de encaminamiento. En este caso, el valor del campo de protección del encabezamiento de paquete no debe cambiarse.

El modelo de encaminamiento alternativo permite garantizar la accesibilidad de la red, pero no la calidad de servicio.

## 9 Mecanismo de coordinación de la protección

Si los nodos están conectados a través de múltiples enlaces agregados y uno o varios de los enlaces agregados fallan, cabe aplicar en primer lugar la protección de enlace y, si este mecanismo falla, iniciar la protección de camino.

Además, conviene prever un tiempo de espera entre las protecciones de las distintas capas a fin de evitar conmutaciones de protección en un sentido y en otro. Por ejemplo, si una RPDTP está basada en una red de transporte (véanse SDH o WDM), la conmutación de protección de la RPDTP no debe iniciarse a menos que el temporizador de espera haya expirado y la condición de defecto (por ejemplo, un fallo de enlace o de nodo en la red de capa de transporte) sigue estando presente en el punto en cuestión.

## 10 Consideraciones relativas a la seguridad

En la presente Recomendación se definen mecanismos que permiten obtener uno o varios trayectos de protección para proteger el trayecto de servicio. Estos mecanismos son útiles para mejorar la seguridad de una RPDTP. Los mecanismos de fiabilidad descritos en la presente Recomendación suponen que tanto el trayecto de servicio como el trayecto de protección se establecen al mismo tiempo y de la misma manera. Dado que la configuración de ambos trayectos se efectúa conforme a los procedimientos característicos de las RPDTP, no se han determinado riesgos adicionales para la seguridad en relación con los mecanismos de fiabilidad descritos en esta Recomendación.

En términos de inestabilidad cuando se aplica la protección, la presente Recomendación ya prevé un tiempo de espera y un mecanismo de coordinación de la protección.

# Apéndice I

## Descomposición en orejas

(Este apéndice no forma parte integrante de la presente Recomendación.)

Una descomposición en orejas D={P0;P1;…;Pr – 1} de un grafo no orientado G=(V,E) es una partición de E en un conjunto ordenado de trayectos simples con bordes disociados P0;P1;…;Pr – 1, denominados orejas, según se indica a continuación:

- P0 es un ciclo simple.
- Pi (i>0) es un trayecto simple cuyos puntos extremos pertenecen a orejas con una numeración inferior y cuyos vértices internos no pertenecen a orejas con una numeración inferior.
- Pi (i>0) también puede ser un ciclo simple. Si se trata de un ciclo con un solo borde, se denomina oreja trivial.

Una descomposición en orejas se denomina abierta única y exclusivamente si no existe un ciclo para Pi (i>0).

En la Figura I.1, la topología de red presentada en la parte izquierda se descompone en cuatro orejas presentadas en la parte derecha. Entre ellas, $P_0$ es un ciclo simple que comprende los nodos 0, 1, 3 y 6; $P_1$ comprende los nodos 2, 4 y 7, con los puntos extremos 3 y 0 pertenecientes a la oreja $P_0$, que es una oreja de numeración inferior en comparación con $P_1$; $P_2$ comprende los nodos 5 y 8, con los puntos extremos 2 y 6 pertenecientes a las orejas $P_1$ y $P_0$, respectivamente, que son orejas de numeración inferior en comparación con $P_2$; $P_3$ comprende el nodo 9, con los puntos extremos 7 y 8 pertenecientes a las orejas $P_1$ y $P_2$, respectivamente, que son orejas de numeración inferior en comparación con $P_3$.

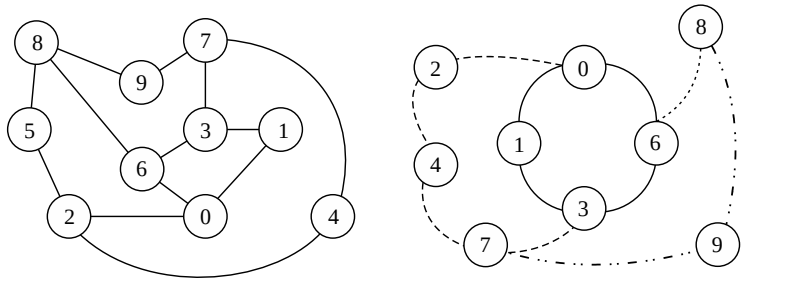


**Figura I.1 – Descomposición en orejas**

La descomposición en orejas sólo puede aplicarse si el grafo es biconexo. En una RPDTP, un grafo biconexo permite garantizar la protección contra fallos en los enlaces o los nodos.

# Bibliografía


[b-UIT-T G.780] Recomendación UIT-T G.780/Y.1351 (2010), *Términos y definiciones para las redes de jerarquía digital síncrona*.

[b-UIT-T G.870] Recomendación UIT-T G.870/Y.1352 (2010), *Términos y definiciones para redes ópticas de transporte*.

[b-UIT-T G.8131] Recomendación UIT-T G.8131/Y.1382 (2007), *Conmutación lineal de protección para las redes MPLS de transporte*.

[b-UIT-T I.322] Recomendación UIT-T I.322 (1999), *Modelo de referencia de protocolo genérico para redes de telecomunicaciones*.

[b-UIT-T I.630] Recomendación UIT-T I.630 (1999), *Conmutación de protección del modo de transferencia asíncrono*.

[b-UIT-T M.2102] Recomendación UIT-T M.2102 (2000), *Procedimientos y umbrales de mantenimiento para los mecanismos de recuperación (protección y restablecimiento) de caminos (trayectos) contenedores virtuales y secciones de múltiplex internacionales en la jerarquía digital síncrona*.

[b-UIT-T X.25] Recomendación UIT-T X.25 (1996), *Interfaz entre el equipo terminal de datos y el equipo de terminación del circuito de datos para equipos terminales que funcionan en el modo paquete y están conectados a redes públicas de datos por circuitos especializados*.

[b-UIT-T X.121] Recomendación UIT-T X.121 (2000), *Plan de numeración internacional para redes públicas de datos*.

[b-UIT-T X.136] Recomendación UIT-T X.136 (1997), *Valores de precisión y de seguridad de funcionamiento para redes públicas de datos que prestan servicios internacionales de conmutación de paquetes*.

[b-UIT-T X.137] Recomendación UIT-T X.137 (1997), *Valores de disponibilidad para redes públicas de datos que prestan servicios internacionales de conmutación de paquetes*.

[b-UIT-T X.200] Recomendación UIT-T X.200 (1994) | ISO/CEI 7498-1:1994, *Tecnología de la información – Interconexión de sistemas abiertos – Modelo de referencia básico: El modelo básico*.

[b-UIT-T X.212] Recomendación UIT-T X.212 (1995) | ISO/CEI 8886:1996, *Tecnología de la información – Interconexión de sistemas abiertos – Definición del servicio de enlace de datos*.

[b-UIT-T X.323] Recomendación UIT-T X.323 (1988), *Disposiciones generales sobre el interfuncionamiento entre redes públicas de datos con conmutación de paquetes (RPDCP)*.

[b-UIT-T X.371] Recomendación UIT-T X.371 (2001), *Disposiciones generales para el interfuncionamiento de redes públicas de datos e Internet*.

[b-UIT-T Y.1001] Recomendación UIT-T Y.1001 (2000), *Marco del protocolo Internet – Marco para la convergencia de tecnologías de redes de telecomunicaciones y de redes de protocolo Internet*.

[b-UIT-T Y.1251] Recomendación UIT-T Y.1251 (2002), *Modelo arquitectural general para el interfuncionamiento*.

[b-UIT-T Y.1720] Recomendación UIT-T Y.1720 (2006), *Conmutación de protección para redes con conmutación por etiquetas multiprotocolo*.

[b-UIT-T Y.2001] Recomendación UIT-T Y.2001 (2004), *Visión general de las redes de próxima generación*.

[b-UIT-T Y.2011] Recomendación UIT-T Y.2011 (2004), *Principios generales y modelo de referencia general de las redes de próxima generación*.

[b-UIT-T Y.2012] Recomendación UIT-T Y.2012 (2010), *Arquitectura y requisitos funcionales de las redes de próxima generación*.

## SERIES DE RECOMENDACIONES DEL UIT-T

| | |
|---|---|
| Serie A | Organización del trabajo del UIT-T |
| Serie D | Principios de tarificación y contabilidad y cuestiones económicas y políticas de las telecomunicaciones/TIC internacionales |
| Serie E | Explotación general de la red, servicio telefónico, explotación del servicio y factores humanos |
| Serie F | Servicios de telecomunicación no telefónicos |
| Serie G | Sistemas y medios de transmisión, sistemas y redes digitales |
| Serie H | Sistemas audiovisuales y multimedia |
| Serie I | Red digital de servicios integrados |
| Serie J | Redes de cable y transmisión de programas radiofónicos y televisivos, y de otras señales multimedia |
| Serie K | Protección contra las interferencias |
| Serie L | Medio ambiente y TIC, cambio climático, ciberdesechos, eficiencia energética, construcción, instalación y protección de los cables y demás elementos de planta exterior |
| Serie M | Gestión de las telecomunicaciones, incluida la RGT y el mantenimiento de redes |
| Serie N | Mantenimiento: circuitos internacionales para transmisiones radiofónicas y de televisión |
| Serie O | Especificaciones de los aparatos de medida |
| Serie P | Calidad de la transmisión telefónica, instalaciones telefónicas y redes de líneas locales |
| Serie Q | Conmutación y señalización, y mediciones y pruebas asociadas |
| Serie R | Transmisión telegráfica |
| Serie S | Equipos terminales para servicios de telegrafía |
| Serie T | Terminales para servicios de telemática |
| Serie U | Conmutación telegráfica |
| Serie V | Comunicación de datos por la red telefónica |
| Serie X | Redes de datos, comunicaciones de sistemas abiertos y seguridad |
| **Serie Y** | **Infraestructura mundial de la información, aspectos del protocolo Internet, redes de próxima generación, Internet de las cosas y ciudades inteligentes** |
| Serie Z | Lenguajes y aspectos generales de soporte lógico para sistemas de telecomunicación |

Impreso en Suiza
Ginebra, 2019