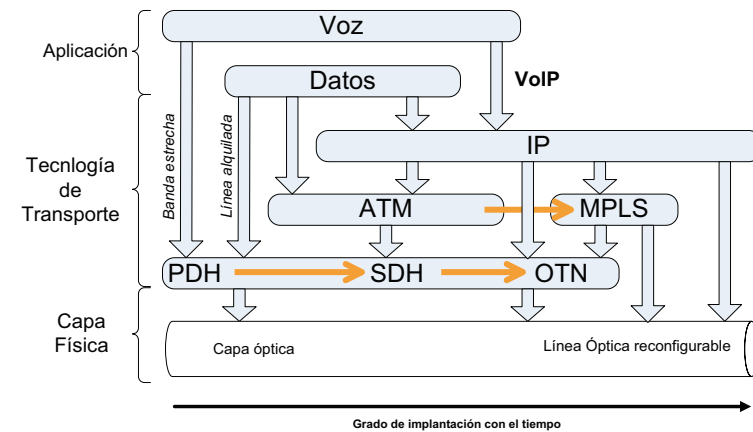


# Tema 0. Introducción a la asignatura

- 0.1. Redes de Acceso y de Transporte
- 0.2. Conmutación y Señalización
- 0.3. Transmisión analógica y digital
- 0.4. Multiplexación
- 0.5. La red telefónica
- 0.6. Transmisión por fibra óptica

## Evolución de las redes de transporte



[ASH01] Ash, D.J., Ferguson, S.P.: "The evolution of the telecommunications transport architecture: from megabits/s to terabits/s". Electronics and Communication Engineering Journal. Vol. 13(1):33-42. 2001.

## Redes de Acceso y de Transporte

### Redes de Telecomunicación

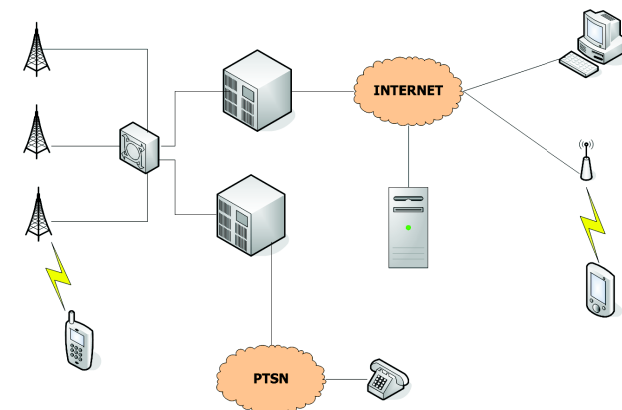
Una red de comunicación está formada por un conjunto de equipos que permiten la transmisión de la información de diferente naturaleza entre diferentes máquinas y la posibilidad de compartir dicha información entre usuarios de la red.

Ejemplos de redes de comunicación son las redes de computadoras o cualquier red de telefonía.

Dentro de una red de comunicación, podemos encontrar diferentes subredes.

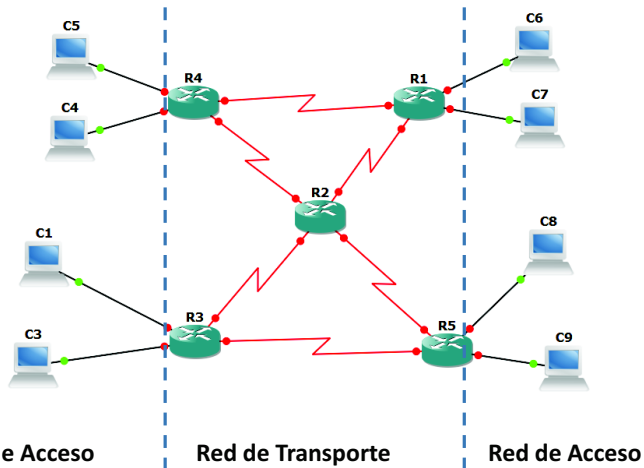
## Redes de Acceso y de Transporte

### Redes de Telecomunicación



# Redes de Acceso y de Transporte

## Redes de Telecomunicación



# Redes de Acceso y de Transporte

## Arquitectura de una red telefónica

Normalmente, las redes se dividen en dos partes:

1) Red de acceso: conecta el usuario con la red

Ejemplo: red de acceso radio en telefonía móvil (UTRAN), Wifi, Bucle de abonado.

2) Núcleo de red (*Back-bone*): que contiene toda la inteligencia de la red, transporta la información a grandes distancias (*long haul*).

En estas redes es necesaria la existencia de una infraestructura que permita transportar la información entre los diferentes equipos.

Ejemplo: conexión entre nodos en UMTS, entre centrales telefónicas, etc.

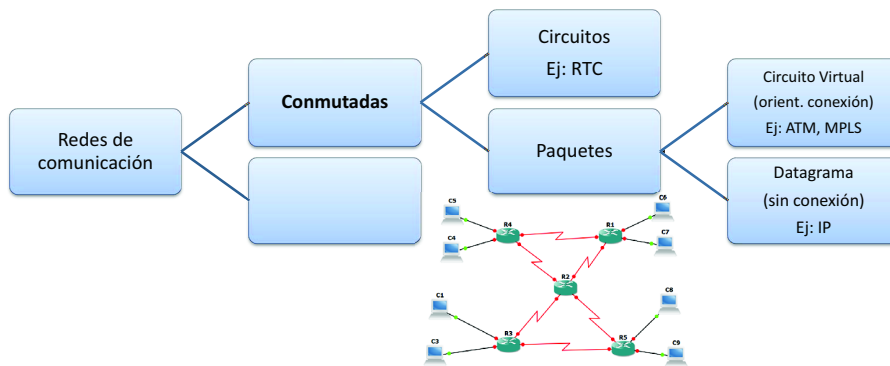
Esta infraestructura la proporcionan las **Redes de Transporte**.

# Redes de Acceso y de Transporte

## Conmutación

Se denomina **conmutación** al establecimiento de una vía de comunicación temporal o permanente entre un emisor y un receptor.

Las redes de transporte son redes conmutadas.



## Redes de Acceso y de Transporte

### ▪ Conmutación de circuitos

Ventajas de la conmutación de circuitos:

- Garantiza un ancho de banda fijo y por tanto una cierta capacidad.
- El retardo es constante.

Desventajas de la conmutación de circuitos:

- El procedimiento de *call setup* introduce un retardo al inicio de la comunicación
- Una vez establecido el canal, el ancho de banda está asignado y no puede ser reutilizado por otro usuario. La compañía cobra por el circuito, aunque no se esté utilizando.

## Redes de Acceso y de Transporte

### ▪ Conmutación de paquetes

- Las redes de conmutación de paquetes utilizan la multiplexación estadística para aprovechar el ancho de banda del canal.
- Los datos se envían en mensajes individuales (paquetes).
- Cada paquete se reenvía al siguiente conmutador hasta llegar al destino
- Cada conmutador tiene un buffer (cola) que permite almacenar temporalmente los paquetes antes de ser reenviados, en el caso de que la línea de salida esté ocupada.

## Redes de Acceso y de Transporte

### ▪ Conmutación de paquetes

Ventajas de la conmutación de paquetes:

- Utilizan los recursos de forma más eficiente (ancho de banda).
- Normalmente no es necesario un procedimiento de call setup
- El usuario sólo paga por el volumen de datos transmitido

Desventajas de la conmutación de paquetes:

- No garantizan un retardo ni capacidad determinados. Aplicaciones de tiempo real, voz o vídeo normalmente no toleran grandes variaciones en los retardos.
- Cuantos más usuarios compartan el canal, el retardo aumenta y el *throughput* disminuye.
- La tarificación es más compleja que en las redes de conmutación de circuitos, ya que hay que contabilizar el volumen de datos transferido por cada usuario de forma individual.

## Redes de Acceso y de Transporte

### ▪ Señalización

Se denomina señalización al mecanismo de transferencia de información de control entre los nodos de una red de telecomunicaciones.

En el (UIT-T Q.9), la señalización se define como:

***Intercambio de información relacionada específicamente con el establecimiento, la liberación y otras formas de control de las comunicaciones, y con la gestión de la red, en la explotación automática de telecomunicaciones.***

## Redes de Acceso y de Transporte

### ▪ Señalización

- Las redes telefónicas primitivas consistían en una serie de líneas conectadas a una central, de modo que sólo proporcionaba servicio de comunicación local a los usuarios conectados a dicha central, dado que estas centrales estaban aisladas unas de otras.
- Posteriormente, comenzaron a interconectarse las centrales entre sí con el fin de ampliar la conectividad con usuarios de otras ciudades o países. Esa red de centrales interconectadas es lo que hoy se denomina red telefónica pública conmutada. (PSTN)
- Estas redes, es necesario la realización de una serie de operaciones para establecer la comunicación entre dos usuarios: determinación del circuito a utilizar, reserva de recursos, liberación de los mismos al terminar la llamada, etc. Es decir, surge la necesidad de un mecanismo de señalización entre los elementos de la red para gestionar los recursos.

## Transmisión analógica y digital

- Se trata de transmitir la información mediante señales analógicas. Dicho de otro modo, la señal que transporta la información es continua.
- El uso de transmisión analógica (o digital) depende del medio.
- Dada la importancia de las redes de telefonía, la transmisión analógica ha dominado las comunicaciones durante mucho tiempo. Hoy en día, se sigue utilizando, por ejemplo para radio sobre fibra.
- Si tomamos como ejemplo la red telefónica analógica, podemos caracterizarla de la siguiente forma:
  - a) Bajo ancho de banda (4KHz). Suficiente para la transmisión de voz.
  - b) Alta tasa de error (comparado con redes digitales como una LAN), que no resulta especialmente importante en comunicaciones analógicas.

## Transmisión analógica y digital

### Pueden transmitirse de forma analógica:

- a) **Datos digitales.** Es necesario transformar los datos digitales a analógicos. El dispositivo encargado de esta tarea se conoce como *modem*. Esta transformación requiere:
  - 1) Generar una portadora en el emisor, que será un tono continuo (ej. 1-2 KHz).
  - 2) Codificar los datos digitales en señales analógicas. Para ello existen diferentes técnicas (ASK, FSK, PSK, QAM)
- b) **Datos analógicos.** Es posible transmitir datos analógicos de forma analógica, modulando la señal (AM, FM, DSB, SSB etc.). La modulación se realiza fundamentalmente por dos razones:
  - Normalmente, no se puede transmitir en banda base
  - Es posible la multiplexación por división de frecuencia

## Transmisión analógica y digital

La transmisión digital tiene ciertas ventajas sobre la transmisión analógica:

- Los circuitos necesarios para la transmisión analógica incluyen amplificadores, cada uno de los cuales añaden ruido y distorsionan la señal.
- Los amplificadores digitales regeneran la señal, eliminándose errores acumulativos (no se amplifica el ruido).

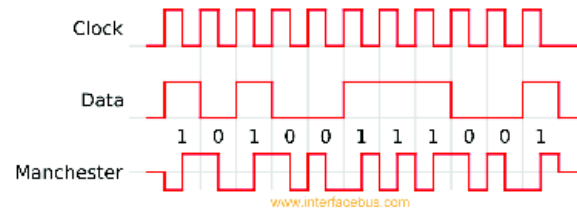
No obstante, la transmisión digital requiere que el emisor y el receptor estén *sincronizados*. El receptor debe ser capaz de determinar la duración de un bit para realizar el muestreo de los datos recibidos. Errores en la sincronización provocan errores en la transmisión y por tanto, pérdida de datos.

# Transmisión analógica y digital

Existen diferentes dos métodos para sincronizar emisor y receptor:

1) Incluir información de temporización en la señal transmitida

Ejemplo: Codificación Manchester



2) Utilizar un canal separado de sincronismo

# Transmisión analógica y digital

Pueden transmitirse de forma digital:

- a) **Datos digitales.** Es necesario codificar la señal e incluir información de sincronismo. Un ejemplo es la codificación Manchester.
- b) **Datos analógicos.** Es necesario convertir la señal analógica a digital. Para ello se utiliza un *codec*.

Muchos sistemas utilizan el codec PCM (Pulse Code Modulation) , que muestrea la señal a la frecuencia de Nyquist.

Con PCM, cada muestra es una medida cuantificada de la amplitud de la señal de n-bits.

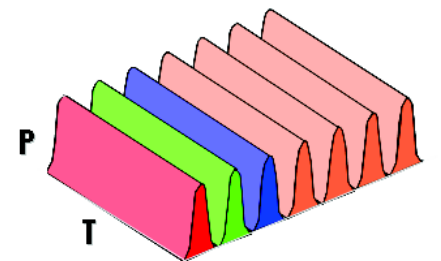
# Multiplexación

Actualmente se dispone de canales de gran capacidad. Dado el elevado coste económico de tender, por ejemplo, una fibra óptica bajo el océano, el canal se divide en canales lógicos que pueden transportar información de usuarios individuales.

Existen diferentes métodos de multiplexación:

# Multiplexación

## ▪ Multiplexación por división de la frecuencia (FDM)



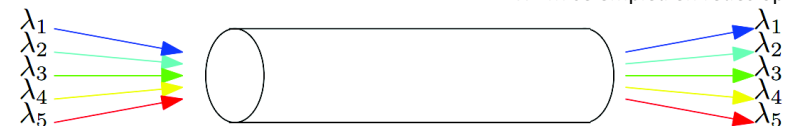
- Divide el espectro disponible en subcanales.

- Cada usuario utiliza una frecuencia (subcanal) de forma exclusiva

- Cuando el usuario no transmite, no es posible reutilizar el ancho de banda para otro usuario

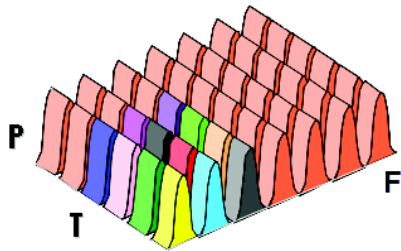
- No siempre aprovecha el ancho de banda disponible

- WDM se emplea en redes ópticas



## Multiplexación

### ▪ Multiplexación por división del tiempo (TDM)

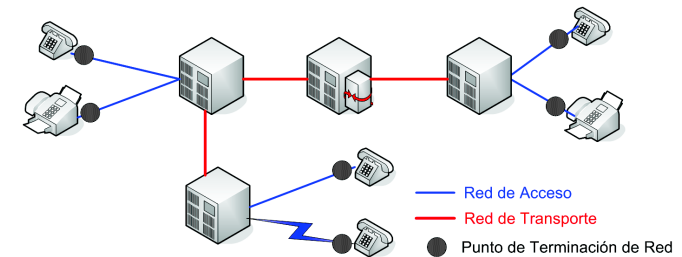


- Divide el tiempo en ranuras
- Cada usuario utiliza todo el ancho de banda disponible pero solo durante un determinado tiempo
- Cuando el usuario no transmite, no es posible reutilizar el ancho de banda para otro usuario
- No siempre aprovecha el ancho de banda disponible
- Es posible combinar FDM y TDM

## La red Telefónica

### ▪ Arquitectura de la RTB

- La conexión telefónica tradicional se realizaba a través de la red telefónica conmutada (RTB).
- Dicha red constaba de tres elementos básicos:
  - Conmutadores
  - Enlaces
  - Equipos terminales (tradicionalmente, teléfonos o fax ⇒ voz).



## La red Telefónica

### ▪ Digitalización de la RTB

La red telefónica conmutada se fue digitalizando en diferentes fases:

1) **Digitalización de la red de transporte:** utilizando multiplexación por división en el tiempo (TDM) y PCM (Pulse Code Modulation), frente a los sistemas de multiplexación en frecuencia (FDM) utilizados anteriormente ⇒ uso de estructuras de bits ⇒ TRAMAS

Voz ocupa unos 4KHz → muestreo a 8KHz. Al usar 8 bits por muestra resultan 64Kbit/s.

2) **Digitalización de las centrales de conmutación:** permitiendo el uso de ciertas características que requieren memoria en el conmutador.

3) **Digitalización de la señalización:** las señales necesarias para el establecimiento, mantenimiento y liberación de una conexión se digitalizan. Actualmente se utiliza el sistema de señalización nº 7 (SS7).

## La red Telefónica

4) **Digitalización del bucle de abonado:** permitiendo a los usuarios acceder a nuevos servicios como la videotelefonía, que no se podrían ofrecer con la tecnología analógica.

Tras estas cuatro fases de digitalización, se dispone ya de una red totalmente digitalizada y compatible con la analógica.

Esta red total o parcialmente digitalizada, pero en la que existe un núcleo digital y la posibilidad de ofrecer un bucle de abonado digital, se conoce como Red Digital de Servicios Integrados.

El ancho de banda de la RDSI depende del número de canales de 64 Kbps contratados, hasta 1920 Kbps.

Posteriormente se introdujo el sistema PDH para añadir capacidad a las redes digitales basadas en tecnología PCM.

# Transmisión por fibra óptica

## ¿ Por qué fibra óptica?

Casi todas las redes de transporte de alta capacidad emplean transmisión por fibra óptica, debido a:

- **Alcance:** La atenuación de una fibra óptica a  $\lambda = 1.55\mu\text{m}$  (192THz) es de 0.2dB/Km. La de un cable coaxial a 1GHz es aprox. 20dB/Km.
- **Ancho de banda:** En fibra actualmente se consiguen 32 portadores x 10Gbit/s (D-WDM), y se está empezando a comercializar tecnología que permite 10 veces más (100GbEthernet - <http://www.ist-mirthe.eu/>).
- **Conmutación y multiplexación óptica:** Se pueden conmutar y multiplexar ópticamente las portadoras ( $\lambda$ ), siendo transparente al formato electrónico de la información.

# Transmisión por fibra óptica

## Principio físico

- Un diodo láser se modula con la señal (digital) de información, generando pulsos luminosos que, tras propagarse por la fibra, se vuelven a convertir en pulsos eléctricos en un fotodetector.



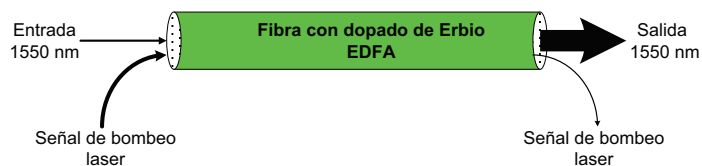
- Para transmitir sobre distancias muy elevadas hace falta regenerar la señal (las 3 Rs):
  - Re-Amplificación (se puede hacer ópticamente)
  - Regeneración del pulso (elimina el ensanchado del pulso)
  - Re-sincronización (recupera el reloj)

} electrónica

# Transmisión por fibra óptica

## Ejemplo de dispositivo óptico

- Para la re-amplificación se emplean "Erbium Doped Fiber Amplifiers" (EDFAs).



- Hasta 20dB de amplificación.

## Tema 1. Señalización. Sistema SS7

- ¿Cómo llega a mi teléfono el número que me llama?
- Cuando llamo a un número 900 cómo sabe la red que:
  - No me debe cobrar
  - El número de teléfono físico al que tiene que dirigir la llamada
- Cuando llamo a un móvil, ¿cómo sabe la red a qué operador tiene que dirigir la llamada? ¿y dónde está el móvil?
- Cuando estoy en Inglaterra, ¿cómo sabe el operador que tengo saldo?

## Tema 1. Señalización. Sistema SS7

### ▪ Índice

1. Introducción
2. Arquitectura de red SS7
3. Tipos de Enlaces SS7
4. Modelo de referencia. Capas
5. MAP
6. SIGTRAN

## La red Telefónica

Inicialmente, la conmutación en las redes telefónicas se realizaba de forma manual, tras la petición de un determinado usuario de comunicarse con otro.



## La red Telefónica

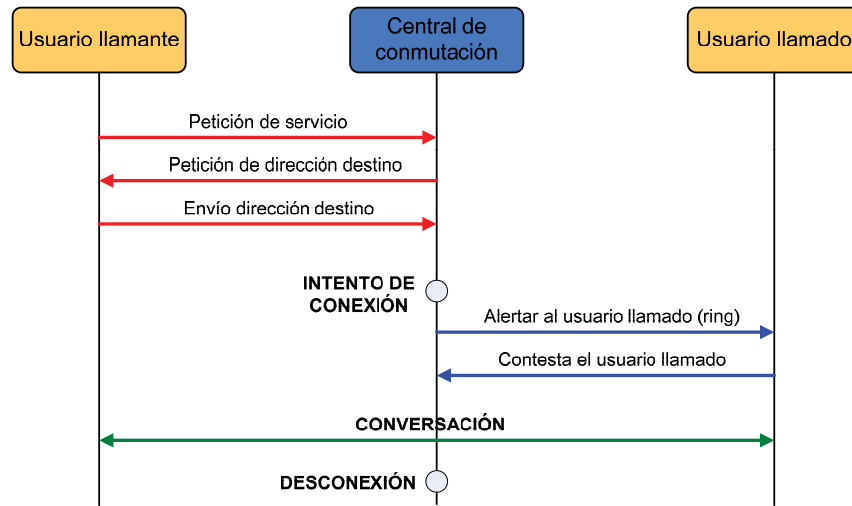
- La operadora realizaba fundamentalmente las siguientes tareas:

- ✓ Cuando el usuario que quiere llamar levanta el teléfono, una indicación luminosa alerta a la operadora
- ✓ La operadora pregunta "¿con quién quiere hablar?"
- ✓ La operadora realiza la conexión con el usuario llamado y su teléfono comienza a sonar
- ✓ Si el usuario llamado descuelga, comienza la comunicación de voz
- ✓ La operadora supervisa la llamada
- ✓ Cuando el usuario cuelga, una indicación luminosa advierte a la operadora la desconexión

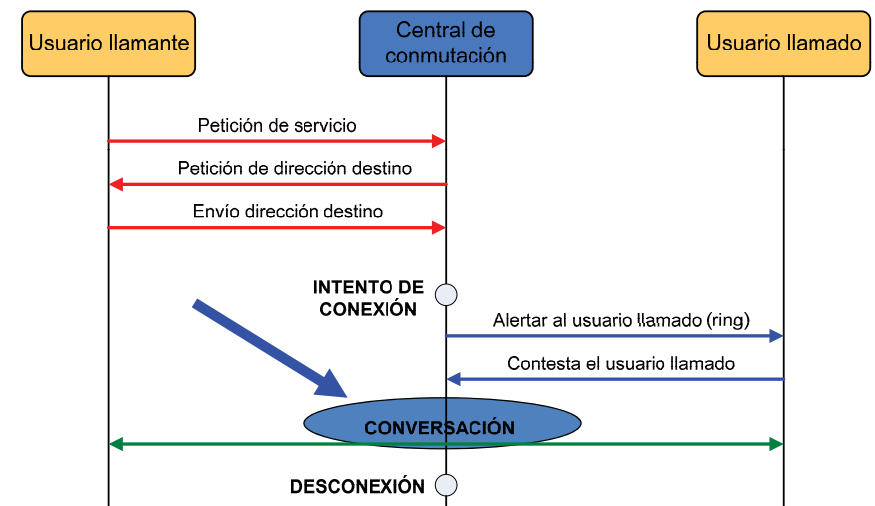




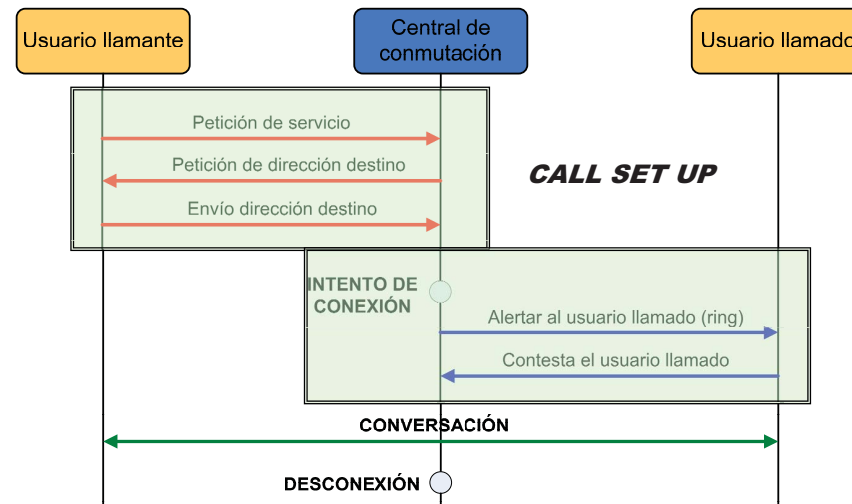
## La red Telefónica



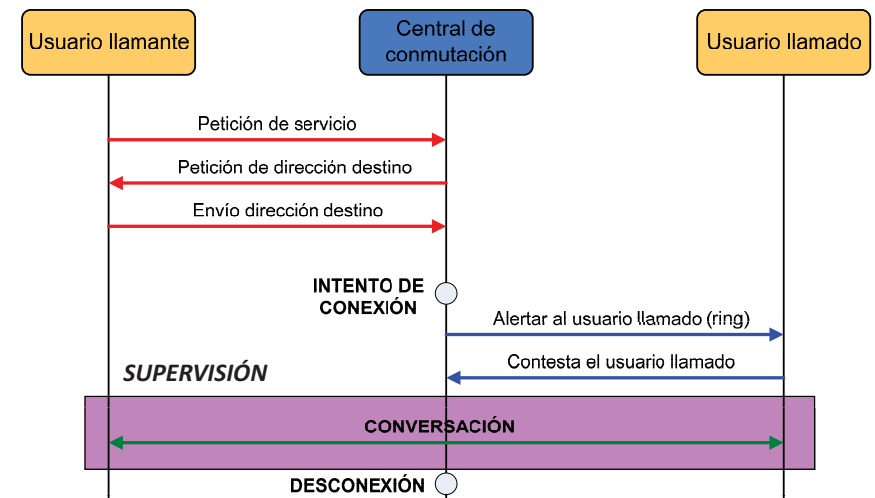
## La red Telefónica



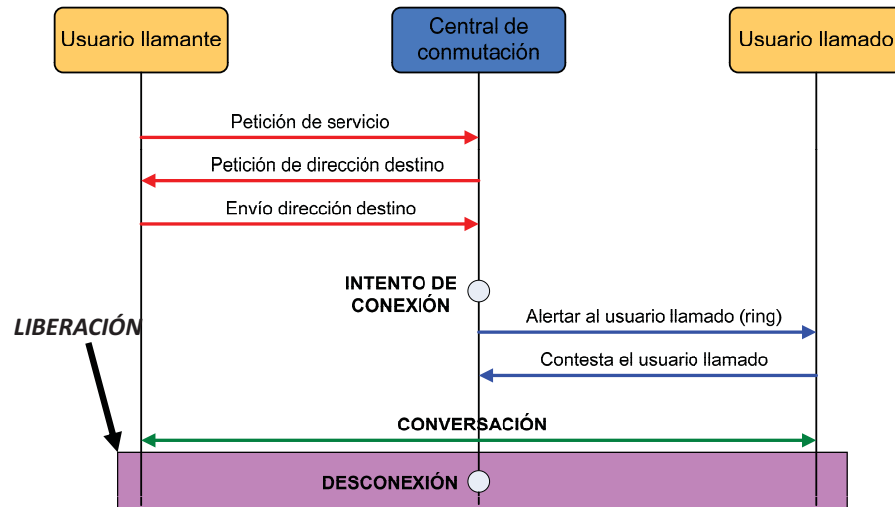
## La red Telefónica



## La red Telefónica



## La red Telefónica



## Señalización en la red Telefónica

- Para implementar las distintas tareas que lleva a cabo la operadora (fundamentalmente, establecimiento, supervisión y liberación de la llamada), se define un conjunto de mensajes de *señalización*.
- Con la digitalización de las redes de telefonía, la tecnología de señalización ha ido mejorando, y la operadora ha sido sustituida por las centrales de conmutación automáticas.
- Esto permite la realización de las mismas tareas de la operadora de una forma más rápida, fiable y eficiente, en una red global en la que intervienen centrales de conmutación de diferentes ciudades, incluso países y en la que intervienen multitud de operadoras de todo el mundo.
- Se han definido diferentes estándares de señalización en diferentes partes del mundo. Aunque las funciones básicas que realizan son las mismas, diferentes sistemas de señalización las llevan a cabo de formas distintas.

## Señalización en la red Telefónica

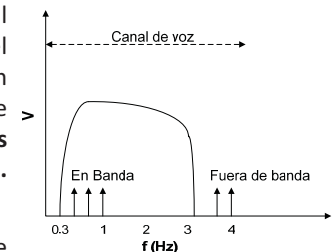
- Centro de conmutación. Centrales 5ESS de Lucent



## Tipos de señalización

- Señalización en banda y fuera de banda

- En banda. Sobre el mismo canal que utiliza el usuario para comunicarse. Suelen utilizarse tonos o secuencias de tonos. El principal problema es que las señales generadas por el usuario pueden confundirse con señalización ocasionando confusiones en los elementos de red. **Es posible enviar mensajes a los elementos de red con fines fraudulentos. Ej. Blueboxes**
- Fuera de banda. Sobre canales adyacentes de bajo ancho de banda. La principal limitación es el reducido número de mensajes distintos soportados.



## Tipos de señalización

### ▪ Señalización en banda y fuera de banda

- Ejemplo de señalización fuera de banda

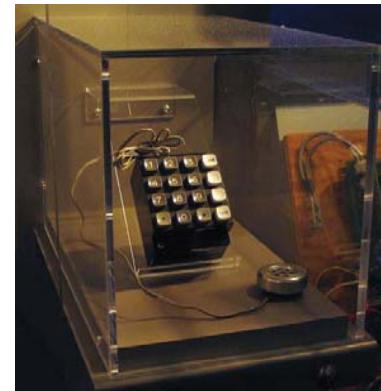


Se utiliza uno de los canales adyacentes para transmitir información de señalización

- Un ejemplo de señalización fuera de banda es el canal D utilizado en la RDSI. Cada usuario tiene un canal D.

## Tipos de señalización

### ▪ Señalización en banda. Problemas de seguridad



**BlueBox**  
www.computerhistory.org

Computer History Museum  
1401 N. Shoreline Blvd  
Mountain View, CA 94043

## Tipos de señalización

- Como se ha comentado, en la actualidad redes de todo el mundo están interconectadas.
- Sin embargo diferentes redes pueden utilizar sistemas de señalización diferentes
- Es por tanto necesario adaptar la señalización ente los diferentes redes.
- Existen dos formas de implementar la señalización en cuanto al canal utilizado:
  - **Canal asociado:** Cada canal de voz (datos) tiene asociado su propio canal de señalización, de uso exclusivo.
  - **Canal común:** La señalización de todas las llamadas se transfiere por el mismo canal de control (SS7).

## Tipos de señalización

### ▪ Señalización por canal asociado

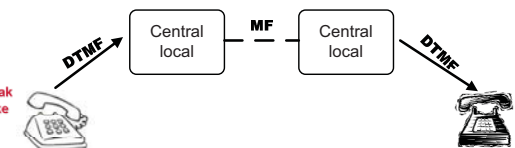
Ejemplo de señalización en banda. Marcado por DTMF

### Tone Dialing

#### Dual Tone Multi-Frequency (DTMF)

	1209	1336	1477	1633
697	1	2	3	A
770	4	5	6	B
852	7	8	9	C
941	*	0	#	D

Timing:  
60 ms Break  
40 ms Make



## Tipos de señalización

### ▪ Señalización por canal asociado (ACS)

- Aunque la señalización por canal asociado es un sistema que se ha utilizado (y se sigue utilizando en algunos casos) durante mucho tiempo y en diferentes países del mundo, presenta ciertos problemas:
  - No es posible enviar mensajes de señalización en ausencia de llamada. Esto provoca cuellos de botella y pérdida de ancho de banda. (Ejemplo: necesito una conexión completa para mandar el tono de “ocupado”).
  - Sólo es viable cuando el tráfico de la red no es muy alto

¿ Por qué?

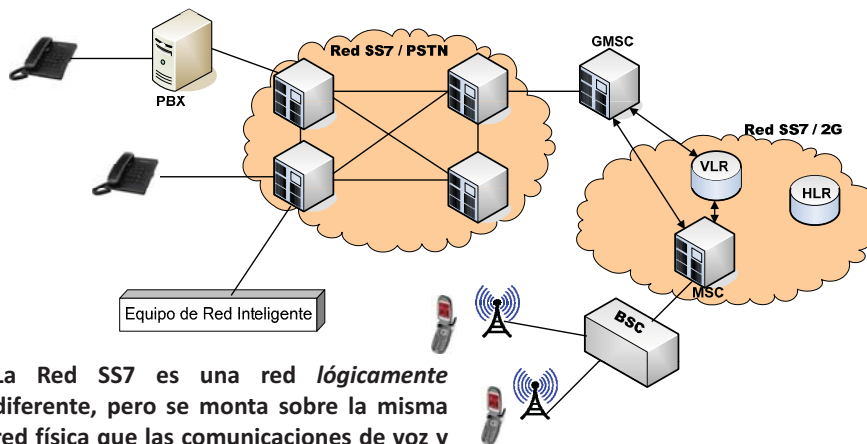
## Tipos de señalización

### ▪ Señalización por canal común (CCS)

- La señalización de todas las llamadas se transfiere por un mismo canal de control (separado del canal que transfiere la voz).
- Los mensajes de señalización han de llevar un identificador del canal al que pertenece la señalización.
- Proporciona una gran capacidad para la definición de mensajes de señalización
- Permite diferenciar información de usuario y de control
- Permite la definición de nuevos servicios suplementarios al servicio telefónico básico tales como la llamada en espera, identificación de número entrante, desvío de llamada, etc.

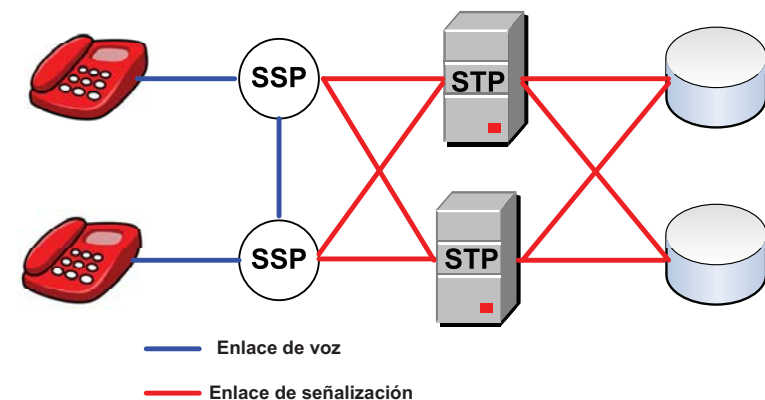
## Señalización SS7

### ▪ Arquitectura de red



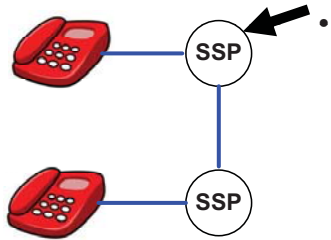
## Señalización SS7

### ▪ Arquitectura de red



## Señalización SS7

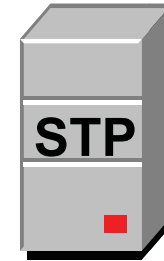
### Arquitectura de red. Nodos de la red SS7



- **SSP (Signaling Switching Point).** Son conmutadores que originan, terminan o encolan llamadas. Un SSP envía mensajes de señalización a otros SSP para establecer, gestionar o liberar los circuitos de voz que son necesarios para completar una llamada. Además, un SSP puede enviar, a través de un STP, peticiones a una base de datos centralizada (SCP) para determinar el encaminamiento de una llamada.

## Señalización SS7

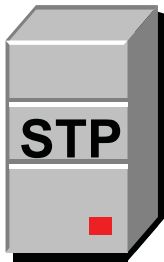
### Arquitectura de red. Nodos de la red SS7



- **STP (Signaling Transfer Point).** Son conmutadores de *paquetes* cuya misión consiste en encaminar el tráfico de señalización de la red.
- Un STP encamina cada mensaje SS7 entrante por uno de los enlaces de salida, utilizando la dirección contenida en el mensaje SS7.
- El STP elimina la necesidad de tener enlaces directos entre cada par de puntos de señalización.

## Señalización SS7

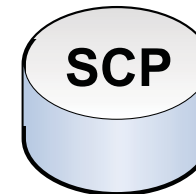
### Arquitectura de red. Nodos de la red SS7



- El STP realiza un procedimiento llamado *global title transform*, mediante el cual, el punto de señalización destino se determina a partir de los dígitos presentes en el mensaje SS7 (por ejemplo, un número 900, un prefijo móvil, etc.).
- Además, un STP actúa como cortafuegos para los mensajes SS7 intercambiados con otras redes.

## Señalización SS7

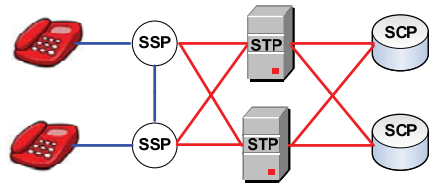
### Arquitectura de red. Nodos de la red SS7



- El **SCP (Service Control Point)** en general, es un componente de lo que hoy se denomina *red inteligente* (IN). Contiene información necesaria para encaminar las llamadas a un punto de señalización destino a partir del número marcado, que es enviada a los SSP bajo petición.

## Señalización SS7

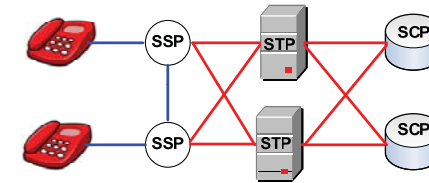
### Arquitectura de red. Nodos de la red SS7



- La red SS7 es crítica para el proceso de establecimiento, mantenimiento y liberación de las llamadas. Dicho de otra forma, los servicios que proporciona una operadora dependen del funcionamiento de la red SS7. Por este motivo, los SCPs y los STPs están duplicados (*mated pairs*) en la red SS7 y ubicados físicamente en sitios diferentes para proporcionar la redundancia necesaria que evite la caída de la red en caso de fallo de uno de estos nodos.
- Los enlaces entre puntos de señalización también se provisionan por pares.

## Señalización SS7

### Arquitectura de red. Nodos de la red SS7

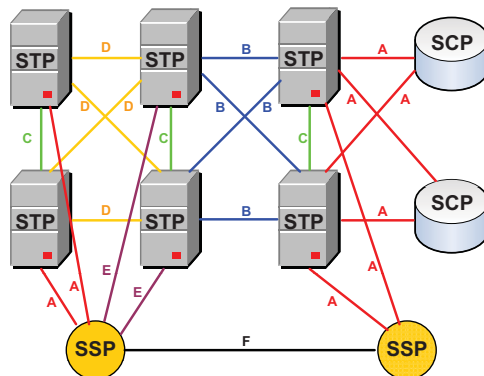


- El tráfico de la red SS7 se distribuye entre los enlaces existentes. En caso de fallo de uno de los enlaces, el tráfico de la red SS7 se re-encamina por otro conjunto de enlaces.
- Cada enlace está diseñado para estar nominalmente al 25%-40% de carga.
- SS7 proporciona mecanismos de corrección de errores y de retransmisión de paquetes.

## Señalización SS7

### Arquitectura de red. Enlaces en la red SS7

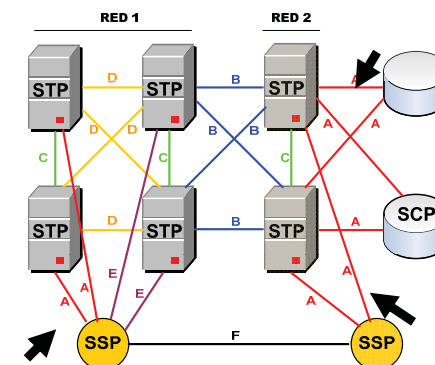
En SS7 se diferencian 6 tipos de enlaces dependiendo del par de equipos que se conecten.



## Señalización SS7

### Arquitectura de red. Enlaces en la red SS7

En SS7 se diferencian 6 tipos de enlaces dependiendo del par de equipos que se conecten.

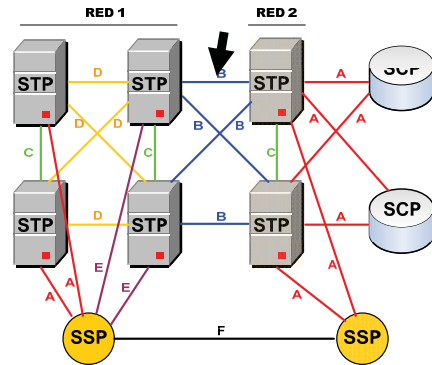


- **Enlace A (Acceso):** conecta dos puntos terminales de señalización (i.e.: un SCP o SSP con un STP). Sólo se transmiten por un enlace A mensajes originados o terminados en un punto terminal de señalización.

## Señalización SS7

### Arquitectura de red. Enlaces en la red SS7

- En SS7 se diferencian 6 tipos de enlaces dependiendo del par de equipos que se conecten.

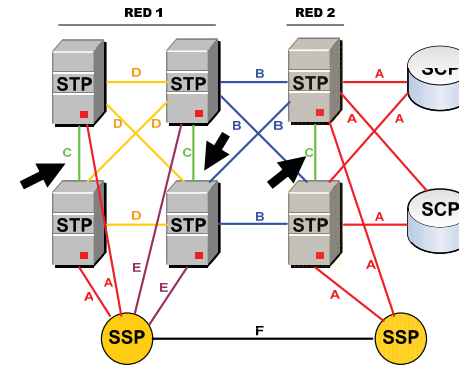


- Enlace B/D (bridge).** Enlace que conecta dos STPs. Es habitual que 4 enlaces B interconecten pares de STP primarios (i.e.: STPs de una red con STPs de otra red). Los enlaces tipo D simplemente se refieren a STP de otra red. Por eso es habitual llamar a estos enlaces B/D.

## Señalización SS7

### Arquitectura de red. Enlaces en la red SS7

- En SS7 se diferencian 6 tipos de enlaces dependiendo del par de equipos que se conecten.



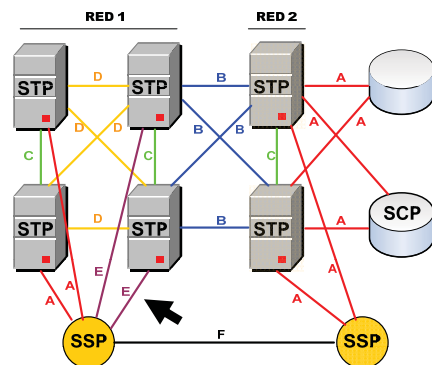
- Enlace C (cross).** Conecta STPs que realizan la misma función, en un par redundante (mated pair). Se utiliza un enlace C (es decir, cursa tráfico de señalización) sólo cuando un STP no tiene otra ruta disponible hacia el punto de señalización destino debido a fallos en los enlaces.

\*\* Nota: aunque los SCPs también se pueden provisionar en pares redundantes, no existe un enlace entre ellos.

## Señalización SS7

### Arquitectura de red. Enlaces en la red SS7

- En SS7 se diferencian 6 tipos de enlaces dependiendo del par de equipos que se conecten.

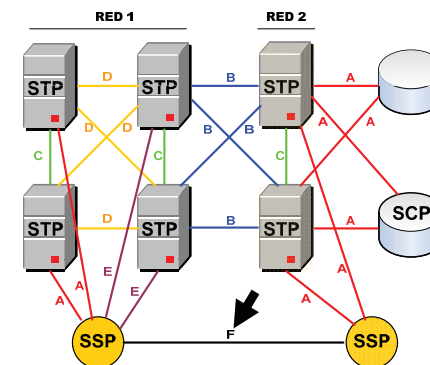


- Enlace E (Extended).** Conecta un SSP con un STP alternativo. Los enlaces E proporcionan un camino de señalización alternativo si no puede alcanzarse el SSP local mediante el enlace A. Normalmente no se provisionan enlaces E a no ser que el beneficio obtenido o que el grado de fiabilidad obtenido justifique el gasto extra que suponen estos enlaces.

## Señalización SS7

### Arquitectura de red. Enlaces en la red SS7

- En SS7 se diferencian 6 tipos de enlaces dependiendo del par de equipos que se conecten.

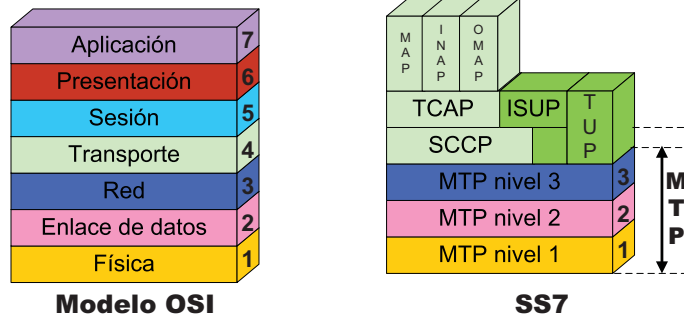


- Enlace F (Fully Associated).** Conecta directamente dos puntos de señalización terminales (i.e.: SSPs y SCPs). Los enlaces F no se utilizan normalmente en redes con STPs.

## Señalización SS7

### Arquitectura de red. Pila de protocolos

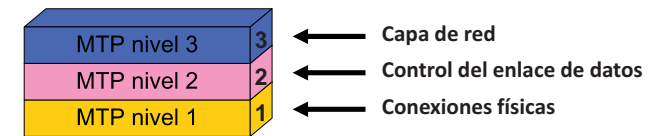
Las diferentes funciones llevadas a cabo por el protocolo SS7 se dividen en diferentes abstracciones funcionales llamadas capas. Esta estructura multicapa se corresponde con las capas del modelo de referencia OSI, aunque algunas de las capas SS7 implementan las funciones de varias capas OSI. (*De hecho SS7 es pre-OSI*).



## Señalización SS7

### Arquitectura de red. Pila de protocolos

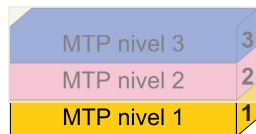
- Como ya se ha visto, la señalización se utiliza fundamentalmente para realizar la gestión automática de las llamadas, a través de un conjunto de mensajes estándar enviados y recibidos por las centrales (puntos de señalización).
- La parte de transferencia de mensajes (MTP) es la responsable del envío de dichos mensajes entre los elementos de la red SS7.
- Toda la red SS7 está construida sobre la MTP, que consiste en tres subcapas



## Señalización SS7

### Arquitectura de red. Pila de protocolos

#### Capa MTP-1

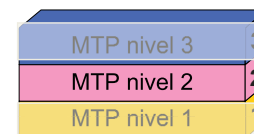


- La capa MTP-1 define el medio físico a través del cual se transfieren los mensajes SS7 de un nodo a otro. Por ejemplo, la capa física puede ser una ranura temporal (*timeslot*) de una trama E1 (2048 kb/s, 32 canales de 64 kb/s).
- Es equivalente a la capa física del modelo OSI y por tanto define las características físicas, eléctricas y funcionales de los enlaces digitales de señalización.

## Señalización SS7

### Arquitectura de red. Pila de protocolos

#### Capa MTP-2



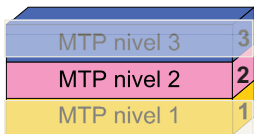
- La capa MTP-2 define el modo en que se utiliza el mecanismo de transferencia de bits MTP-1 para transferir mensajes de longitud variable entre dos nodos.
- Utiliza delimitadores para indicar el inicio o fin de una trama y tiene mecanismos de relleno de bits así como de protección frente a errores para la trama completa, gracias a la inclusión de un CRC al final de la misma. También implementa control de flujo y validación del número de secuencia.



## Señalización SS7

### ▪ Arquitectura de red. Pila de protocolos

#### Capa MTP-2



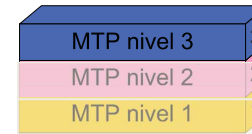
- MTP-2 no aporta nada al contenido del mensaje. Sólo define el mecanismo para que mensajes de cualquier longitud puedan enviarse de manera fiable (libre de errores) entre dos nodos SS7 y puedan ser utilizados por las capas superiores.
- MTP-2 Es equivalente a la capa de enlace de datos del modelo OSI.

**¿Por qué otra tecnología se podrían sustituir las capas MTP-1 y MTP-2?**

## Señalización SS7

### ▪ Arquitectura de red. Pila de protocolos

#### Capa MTP-3



- Proporciona capacidad de encaminamiento de mensajes entre puntos de señalización en la red SS7. Además, MTP-3 re-encamina mensajes lejos de enlaces con fallos y controla el tráfico en situaciones de congestión.
- Cada nodo tiene asignada una dirección única en la red (conocida como Signaling Point Code o SPC).
- MTP-3 puede utilizar múltiples caminos en paralelo desde el SPC a DPC (Destination Point Code) a través de la red, teniendo en cuenta la carga de los enlaces y su disponibilidad (siempre debe haber más de un camino para llegar de un origen SPC a un destino DPC).
- La capa MTP-3 es *equivalente a IP pero emplea encaminamiento estático*.
- Point code ~ Dirección IP

## Señalización SS7

### ▪ Mensajes SS7. Estructura de las tramas

- Los paquetes en la red SS7 se denominan Unidades de Señalización (Signal Units, SU).
- Existen 3 tipos de Unidades de Señalización. La información enviada a través de la red SS7 utiliza uno sólo de los tipos de SU, mientras que las operaciones de gestión de la red SS7 utilizan los 3 tipos de mensajes.
- Hay que tener en cuenta, que a diferencia de otras redes, SS7 está pensada para transferir información entre máquinas y no entre usuarios.
- Las unidades de señalización recaen en cada una de las tres capas MTP, proporcionando encaminamiento, control del enlace y control de errores.

## Señalización SS7

### ▪ Tipos de mensajes SS7. Unidades de Señalización

- Los paquetes en la red SS7 se denominan Unidades de Señalización (Signal Units, SU).
  - FISU: Fill in signal unit
  - LSSU: Link state signal unit
  - MSU: Message signal unit.
- Las FISU se mandan sólo cuando el enlace de otro modo estaría desocupado. Llevan un CRC que permite verificar la calidad de enlace en todo momento, lo que ayuda a detectar fallos lo antes posible y aumentar la fiabilidad.
- Las LSSU monitorizan el alineamiento de las tramas así como el estado de los equipos de señalización en ambos extremos del enlace. Sólo se producen cuando se conecta el enlace (alineamiento de trama inicial) o cuando se producen errores en los equipos. Tienen prioridad sobre los demás.
- MSU: transportan la info de los protocolos de nivel superior. Son los únicos que pueden atravesar la red (FISU y LSSU no "salen" de su enlace).

# Señalización SS7

## Tipos de mensajes SS7

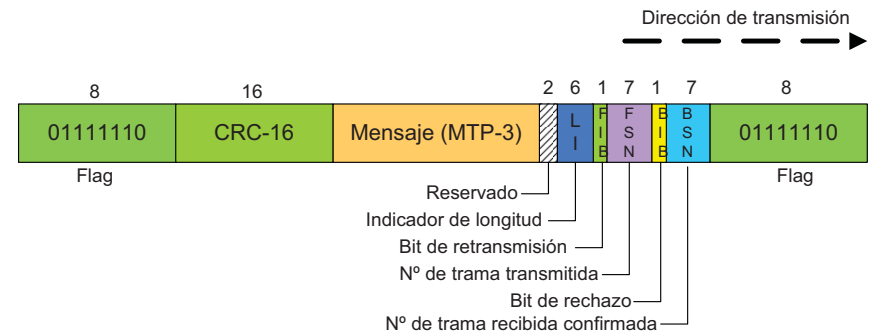
1) **Message Signal Unit (MSU).** Las MSU portan la información en la red SS7.

Una MSU consiste en campos del protocolo MTP y dos campos adicionales:

- a) *Service Indicator Octet (SIO).* Indica el tipo de protocolo de nivel 4 (ej.: TUP, ISUP, etc.)
- b) *Service Information Field (SIF).* Contiene información de control así como 3 etiquetas de encaminamiento. El campo SIF puede contener hasta 272 bytes y se utiliza en los 4 niveles de la pila de protocolos.

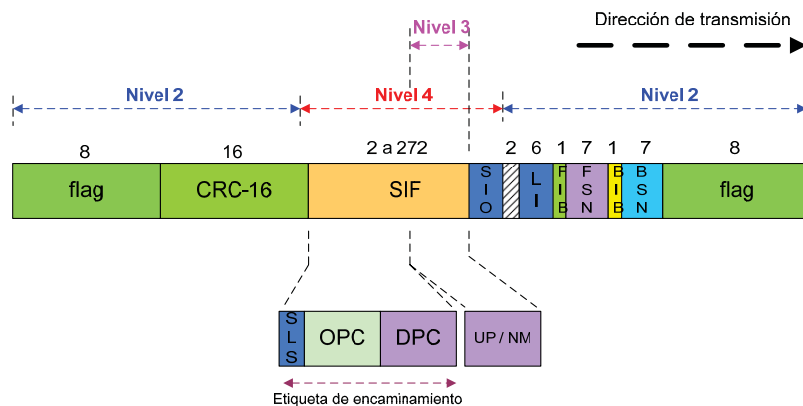
# Señalización SS7

## Formato tramas MSU - MTP-2



# Señalización SS7

## Formato tramas MSU - MTP-3



# Señalización SS7

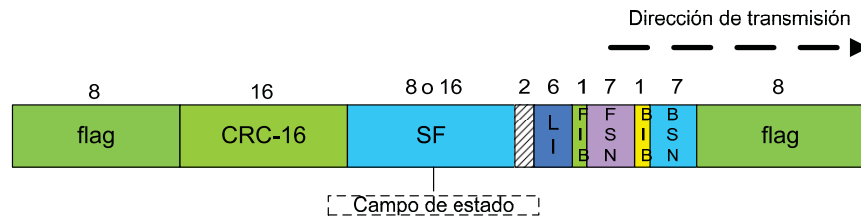
## Tipos de mensajes SS7

2) **Link Status Signal Unit (LSSU).**

- Los mensajes LSSU se utilizan para transportar información sobre el estado de la red.
- Se utilizan en el nivel 3 de un nodo para transmitir información sobre su estado al nodo adyacente.
- Los mensajes LSSU sólo se utilizan en enlaces punto a punto, nunca se transfieren a través de la red (es decir, utilizando más de un nodo SS7).
- Cuando se transfieren mensajes LSSU, se deja de transmitir otro tipo de información (es decir, los mensajes LSSU tiene prioridad sobre los demás).

## Señalización SS7

### ▪ Mensajes SS7. Formato mensajes LSSU



## Señalización SS7

### ▪ Tipos de mensajes SS7

#### 3) Fill-In Signal Unit (FISU).

- Los mensajes FISU se utilizan cuando no hay información que transmitir y la red está “en reposo”.
- FISU se utiliza para monitorizar tasa de error en los enlaces. Esto hace que SS7 sea una red muy fiable, dado que es posible detectar fallos en la red (a través de la monitorización de la calidad de los enlaces) incluso cuando no se está transmitiendo información.
- Además de la monitorización realizada mediante mensajes FISU, el protocolo MTP está constantemente monitorizando el estado de los enlaces de red.

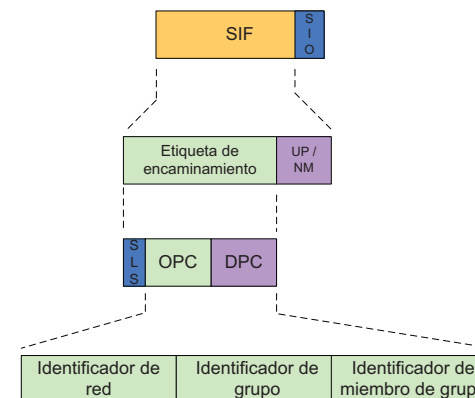
## Señalización SS7

### ▪ Encaminamiento en SS7

- El encaminamiento en las redes SS7 se realiza a nivel MTP-3 y está basado en el punto de señalización destino (DPC)
- Hay dos formas de implementar el encaminamiento:
  - a) DCP que identifica un PS no local → no es necesario invocar SCCP (no es necesaria traducción de direcciones)
  - b) DPC que identifica un PS parcialmente → es necesario invocar la capa SCCP para traducir la dirección.

## Señalización SS7

### ▪ Encaminamiento en SS7. Etiqueta de encaminamiento

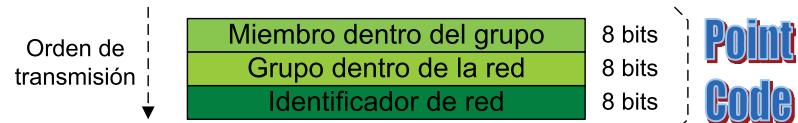


#### Signaling Link Selection (SLS)

- Se utiliza para distribuir el tráfico entre los puntos de señalización adyacentes mediante la selección del enlace apropiado.
- Está formado por 5 bits
- El LSB identifica el link set y los 4 restantes el enlace.
- En el caso de que haya un solo enlace, el LSB se ignora.
- El balanceo de carga se consigue rotando a la derecha los bits en el SLS

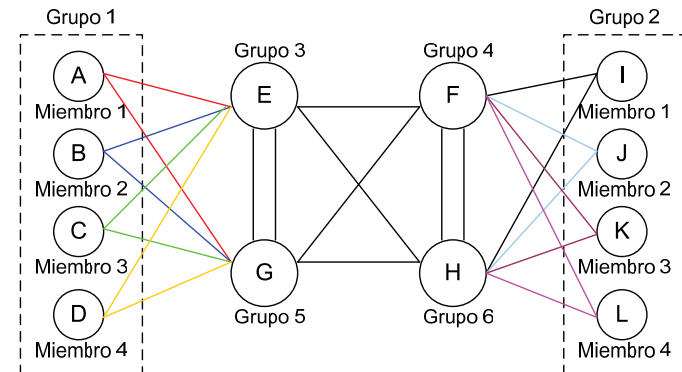
# Señalización SS7

## Encaminamiento en SS7. Identificadores de red



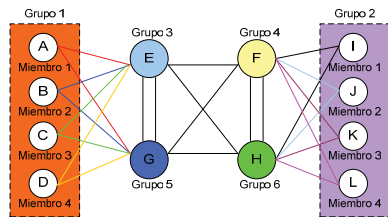
# Señalización SS7

## Encaminamiento en SS7.



# Señalización SS7

## Encaminamiento en SS7.



	PS	Red	Grupo	Miembro
A	0000	0011	0000	0001
B	0000	0011	0000	0001
C	0000	0011	0000	0001
D	0000	0011	0000	0001
E	0000	0011	0000	0011
F	0000	0011	0000	0100
G	0000	0011	0000	0101
H	0000	0011	0000	0110
I	0000	0011	0000	0010
J	0000	0011	0000	0010
K	0000	0011	0000	0010
L	0000	0011	0000	0010

# Señalización SS7

## Encaminamiento en SS7. Ejemplo para el nodo I

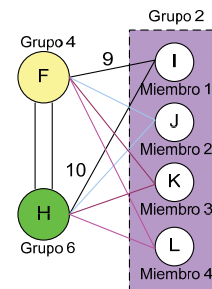


Tabla de red		
Red	Ruta	Ruta alternativa
0000 0011	Puntero a la tabla de grupos	-
Otra	9	10

Tabla de grupos		
Grupo	Ruta	Ruta alternativa
0000 0011	9	10
0000 0110	10	9

## Señalización SS7

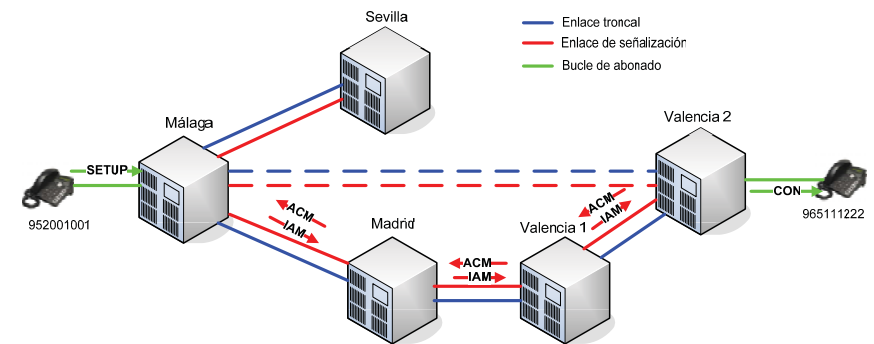
### ▪ Aplicación del encaminamiento. Método *Pass-along* para gestión del tráfico de voz

- SS7 proporciona mecanismos de gestión del tráfico para garantizar la entrega de los paquetes a su destino, siendo tolerante a fallos en los enlaces de señalización. Para ello, se implementan las siguientes funciones a través del envío de mensajes.
  - 1) Paso a enlace de reserva
  - 2) Retorno a servicio
  - 3) Reencaminamiento forzado (búsqueda de rutas alternativas)
  - 4) Reencaminamiento controlado (reactivación o restricción de rutas)
  - 5) Rearranque de la MTP (reactivación de un punto de señalización)

- 1) Paso a enlace de reserva
- 2) Retorno a servicio
- 3) Reencaminamiento forzado (búsqueda de rutas alternativas)
- 4) Reencaminamiento controlado (reactivación o restricción de rutas)
- 5) Rearranque de la MTP (reactivación de un punto de señalización)

## Señalización SS7

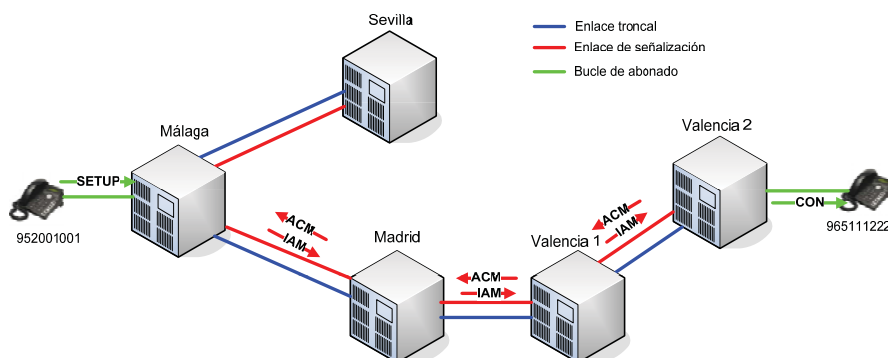
### ▪ Encaminamiento *Pass-along*. Gestión del tráfico de voz



¿ Qué es un circuito de voz a nivel físico ?

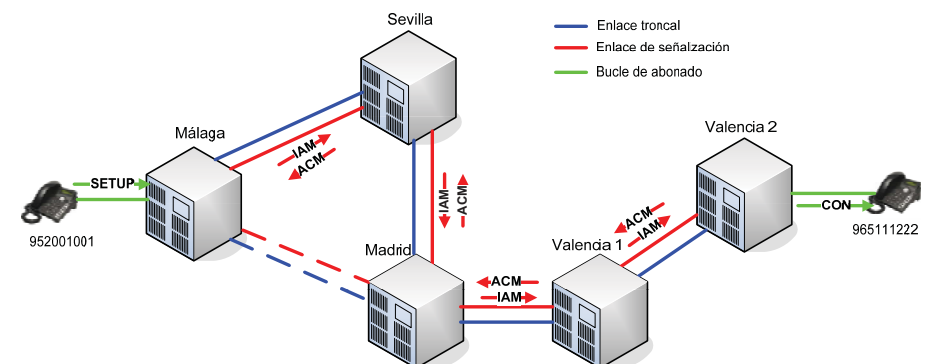
## Señalización SS7

### ▪ Encaminamiento *Pass-along*. Gestión del tráfico de voz



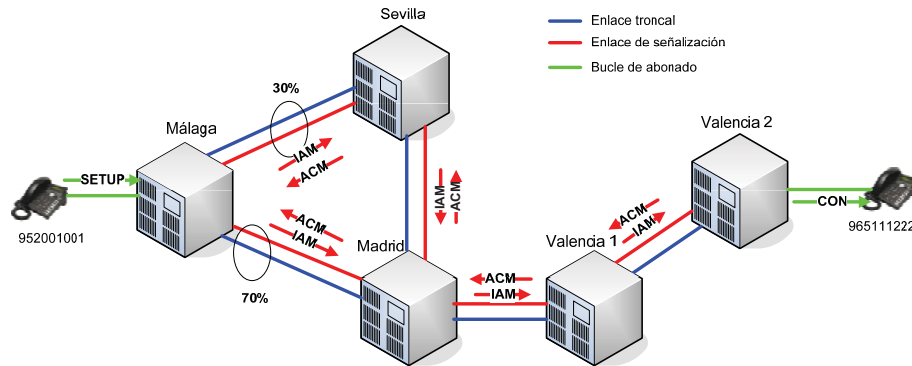
## Señalización SS7

### ▪ Encaminamiento *Pass-along*. Gestión del tráfico de voz



## Señalización SS7

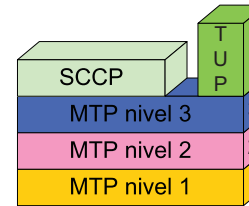
### Encaminamiento *Pass-along*. Balanceo de enlaces



## Señalización SS7

### Telephone User Part (TUP)

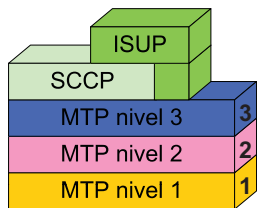
- La capa TUP se utiliza para establecer una llamada telefónica entre dos nodos SS7. Define un conjunto de mensajes y un protocolo utilizando dichos mensajes que permite la gestión de las llamadas telefónicas.
- Los mensajes TUP se envían sólo inmediatamente antes de que la llamada se establezca e inmediatamente antes de que se libere. No hay intercambio de mensajes TUP durante la llamada.
- TUP fue uno de los primeros protocolos dentro de SS7, diseñado para soportar teléfonos analógicos.
- Sustituido por ISUP en la mayor parte del mundo.



## Señalización SS7

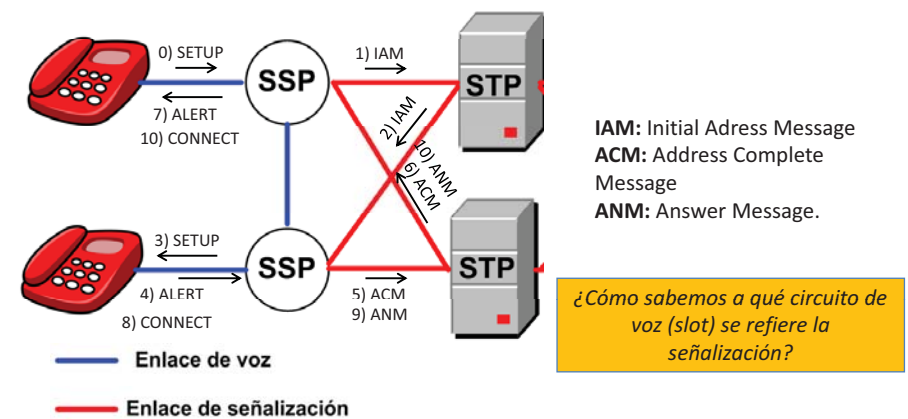
### Integrated Services User Part (ISUP)

- La capa ISUP realiza las mismas funciones que la capa TUP (es decir, establecer y liberar llamadas).
- No obstante es mucho más compleja que la capa TUP, ya que proporciona la funcionalidad sobre enlaces primarios RDSI.
- Esta funcionalidad incluye identificación de número llamante, capacidad de tarificación y otras funciones avanzadas de telefonía, ya que el canal de voz puede utilizarse también para transferir fax o datos.
- Igual que los mensajes TUP, los mensajes ISUP sólo se envían en la fase de establecimiento y liberación de la llamada.
- ISUP sobre SCCP: Para señalización extremo a extremo.



## Señalización SS7

### Ejemplo llamada ISUP



## Señalización SS7

### ▪ Ejemplo llamada ISUP (RDSI) - Establecimiento

- En el procedimiento de establecimiento de llamada en RDSI, se utilizan 3 mensajes SS7 de la capa ISUP: IAM (Initial Address Message), ACM (Address Complete Message) y ANM (Answer Message).
- 1) La información necesaria en para el establecimiento de la llamada la envía el usuario llamante al primer conmutador en un mensaje SETUP. Este mensaje contiene información relativa a la dirección destino así como información de encaminamiento y tratamiento de la llamada.
  - 2) En el primer conmutador, el mensaje SETUP se traduce en un mensaje IAM que es enviado hacia los conmutadores intermedios, indicando la dirección destino (número llamado). Cada conmutador que recibe el mensaje IAM inicia un temporizador (T7). En el caso de que dicho temporizador expire antes de recibir el mensaje ACM, la conexión se libera y se envía una señal al abonado que ha demandado el servicio (llamante).

## Señalización SS7

### ▪ Ejemplo llamada ISUP (RDSI) - Establecimiento

- 3) Cuando un mensaje IAM es recibido por un conmutador intermedio, éste selecciona un circuito libre a partir del número destino y del tipo de servicio demandado. A continuación, envía otro mensaje IAM al siguiente conmutador.
- 4) Cuando el conmutador destino recibe el mensaje IAM, analiza el número solicitado (contenido en IAM) y determina el usuario con el que debe realizar el intento de conexión. También verifica el estado de la línea (ocupada, saturada, etc.) para determinar si es posible la conexión.
- 5) Si la conexión es posible, el conmutador destino envía un mensaje SETUP al usuario llamado.
- 6) Una vez que el usuario llamado recibe el mensaje SETUP, éste envía un mensaje ALERTING al conmutador destino, indicando que el teléfono está sonando.

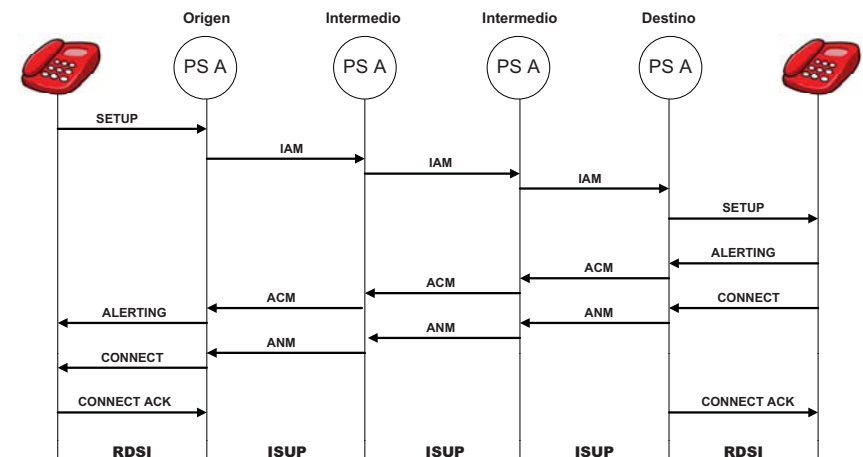
## Señalización SS7

### ▪ Ejemplo llamada ISUP (RDSI) - Establecimiento

- 7) El conmutador destino traduce el mensaje ALERTING en un mensaje ACM (dirección completa) que llega hasta el origen para indicar al usuario llamante que el teléfono destino está sonando.
- 8) La recepción de un mensaje ACM detiene el temporizador T7 y activa otro temporizador (T9), a la espera de un mensaje ANM. Si el temporizador T9 expira antes de recibir el mensaje ACM, la conexión se libera, igual que ocurre con el temporizador T7.
- 9) Cuando el usuario llamado descuelga, se envía un mensaje CONNECT al conmutador destino, que envía un mensaje ANM hacia el conmutador origen y detiene el temporizador T9 en los nodos.
- 10) Una vez que el mensaje ANM llega al conmutador origen, este lo traduce en un mensaje CONNECT que envía al usuario llamante.
- 11) El usuario llamante responde con un CONNECT ACK al nodo origen.

## Señalización SS7

### ▪ Ejemplo llamada ISUP (RDSI)



## Señalización SS7

### ▪ Ejemplo llamada ISUP (RDSI) - Liberación

- En el procedimiento de liberación de llamada en RDSI, se utilizan 2 mensajes SS7 de la capa ISUP: REL (Release), RLC (Release Complete).
  - En el ejemplo, suponemos que el usuario llamante decide colgar.
- 1) El usuario llamante envía un mensaje DISC al nodo origen, que libera el circuito en los dos sentidos.
  - 2) El nodo origen envía un mensaje REL a los nodos intermedios y activa dos temporizadores (T1 y T5). Si no se recibe mensaje RLC en respuesta al mensaje REL antes de que expire T1, el nodo retransmite el mensaje REL.
  - 3) Una vez enviado el primer mensaje REL, el nodo activa el temporizador T5.

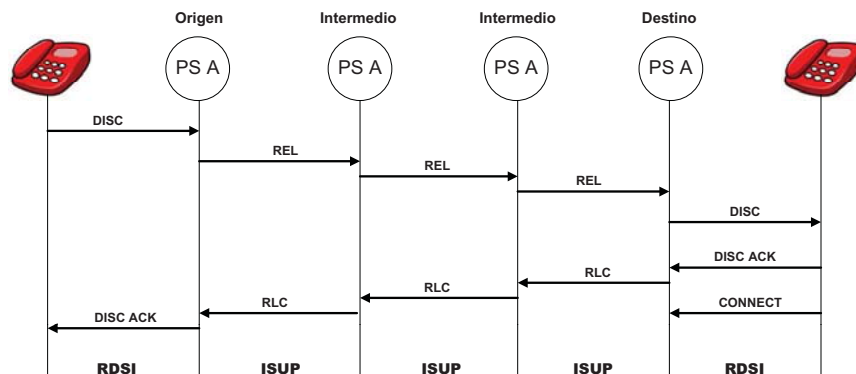
## Señalización SS7

### ▪ Ejemplo llamada ISUP (RDSI) - Liberación

- 4) Si no recibe un mensaje RLC antes de que T5 expire, éste realiza las siguientes acciones:
  - a) Emite un mensaje de inicialización de circuito (RSC, Reset Circuit)
  - b) Emite una alarma al sistema OSS
  - c) Desactiva el circuito
  - d) Emite un mensaje RSC periódico cada vez que expire T5, hasta que intervenga mantenimiento.
- 5) Cuando el nodo destino recibe el mensaje REL, libera el circuito y envía un mensaje DISC al usuario llamado. Además, envía un mensaje RLC a los conmutadores intermedios para que detengan los temporizadores T1 y T5 .

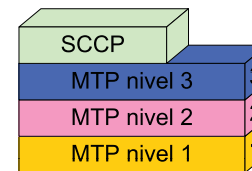
## Señalización SS7

### ▪ Ejemplo llamada ISUP (RDSI) - Liberación



## Señalización SS7

### ▪ Signaling Connection Control Part (SCCP)



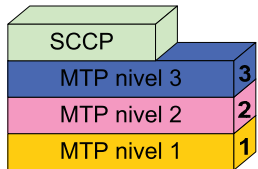
- Proporciona servicios de capa de transporte, tanto orientados como no orientados a conexión para la capa TCAP. Se emplea para transmitir señalización que no está relacionada con el establecimiento de circuitos.
- Implementa la traducción del título global (GTT)



# Señalización SS7

## ▪ Signaling Connection Control Part (SCCP)

Servicios de capa de transporte:



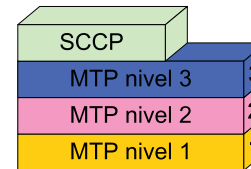
- Permite identificar aplicaciones dentro de un nodo mediante el nº de subsistema (el equivalente a un puerto o socket).
- Puede ser:
  - No orientado a conexión que garantiza la entrega ordenada de los mensajes
  - Orientado a conexión.

SCCP proporciona los servicios suplementarios a la MTP para soportar los servicios de red en modo conectado y en modo no conectado entre nodos SS7. MTP 3 sólo proporciona servicios en modo no conectado.

# Señalización SS7

## ▪ Signaling Connection Control Part (SCCP)

Traducción de Título Global (GT).



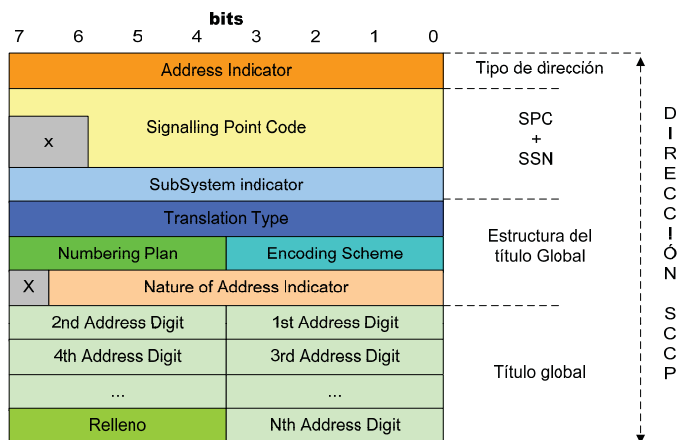
- Un título global (GT) es una dirección (número 900, número RDSI) que no contiene información que permite su enrutamiento explícito en SS7. La capa SCCP realiza la traducción del GT en un número SS7.
- SCCP está implementada en los STP. Por tanto, los puntos de señalización origen (SSP) no necesitan conocer el punto de señalización destino (DPC) ni el número de subsistema del servicio asociado.

**Ejemplo de GTT:** Para comprobar si una tarjeta telefónica tiene saldo, hay que acceder al SCP de la compañía que la emitió.

# Señalización SS7

## ▪ Signaling Connection Control Part (SCCP)

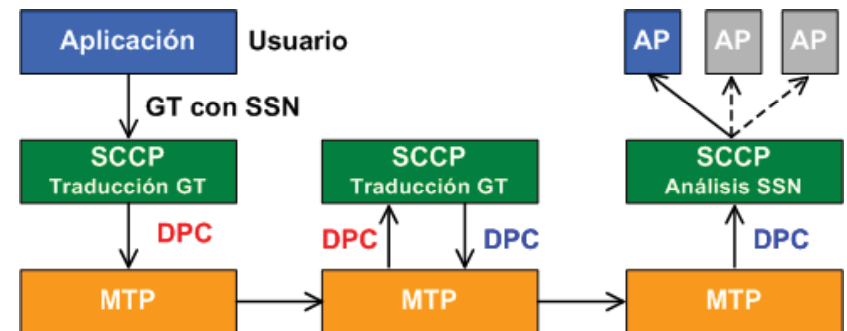
### ▪ Estructura del Título Global



# Señalización SS7

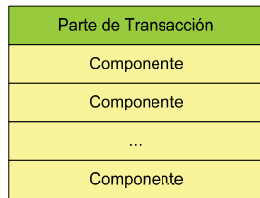
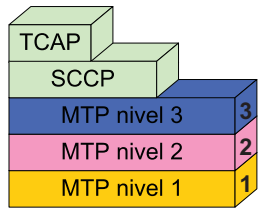
## ▪ Signaling Connection Control Part (SCCP)

### ▪ Traducción de direcciones



## Señalización SS7

### Transaction Capabilities Connection Part (TCAP)

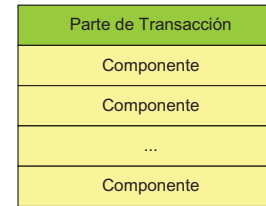


- Corresponde a la capa OSI de Sesión
- La capa TCAP permite el desarrollo de servicios de *red inteligente* mediante el intercambio de elementos de información predefinidos entre puntos de señalización. (Por ejemplo: re-llamada automática, SMS).
- Los 'diálogos' entre aplicaciones se llevan a cabo en forma de transacciones. Cada transacción contiene una serie de 'componentes': invocar, devolver resultado, devolver error, rechazar. (Es parecido a un RPC – remote procedure call)
- Emplea el transporte no orientado a conexión de SCCP.

## Señalización SS7

### Transaction Capabilities Connection Part (TCAP)

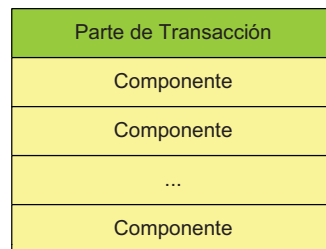
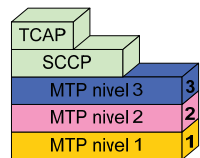
- Los mensajes TCAP están contenidos dentro de la parte SCCP de una MSU (Message Signaling Unit). Un mensaje TCAP está formado por dos partes:



- **Operación.** Es una acción que debe ejecutar el extremo remoto. Está definida en la capa de usuario (encima de TCAP)
- **Componente.** Es la estructura que transporta la petición y las respuestas de una operación.

## Señalización SS7

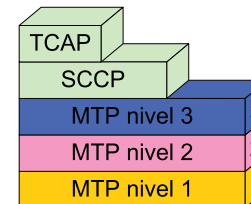
### Transaction Capabilities Connection Part (TCAP)



- Cada transacción tiene un identificador único (TransactionID)
- En una transacción se pueden realizar varias operaciones
- Cada operación tiene un identificador único (InvokeID) que va incluido en todas las componentes de la operación.

## Señalización SS7

### Transaction Capabilities Connection Part (TCAP)



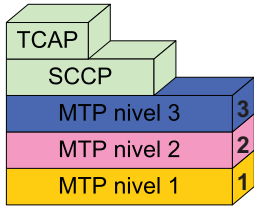
- 1) **Parte de Transacción.** Contiene el identificador de paquete., así como identificadores del origen y destino de la transacción, los cuales asocian la transacción TCAP con una aplicación específica en los SSP origen y destino. Hay 7 tipos de identificadores:
  - a) Unidireccional. Transfiere componentes en una sola dirección.
  - b) Petición con permiso. Inicia una transacción TCAP. El nodo destino puede finalizar la transacción.
  - c) Petición sin permiso. Inicia una transacción TCAP. El nodo destino no puede finalizar la transacción.

## Señalización SS7

### ▪ Transaction Capabilities Connection Part (TCAP)

1) **Parte de Transacción.** Contiene el identificador de paquete. Hay 7 tipos de identificadores:

- d) Respuesta. Finaliza la transacción TCAP
- e) Conversación con permiso. Continúa una transacción TCAP. El nodo destino puede finalizar la transacción.
- f) Conversación sin permiso. Continúa una transacción TCAP. El nodo destino no puede finalizar la transacción.
- g) Abortar. Finaliza la transacción TCAP en una situación anormal.



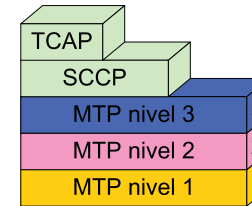
➤ **Dentro de una transacción se pueden producir varias operaciones y cada operación puede tener varios componentes.**

## Señalización SS7

### ▪ Transaction Capabilities Connection Part (TCAP)

2) **Parte de Componentes.** Los componentes incluyen parámetros que contienen datos específicos de la aplicación (no examinados por la capa TCAP). Hay 6 tipos de componentes:

- a) Invocación (*invoke*). Solicita una operación, por ejemplo, una transacción de petición con permiso de la traducción de un número 900 al SCCP. El componente es el último componente en la petición.
- b) Retornar resultado (*return result*). Devuelve el resultado de una operación invocada e indica que dicha operación ha sido completada con éxito. El resultado puede necesitar de más de una componente para ser transmitido.

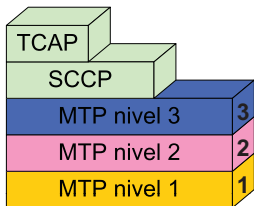


## Señalización SS7

### ▪ Transaction Capabilities Connection Part (TCAP)

c) Error de retorno (*Return Error*). Indica que la operación invocada no se ha completado con éxito. Contiene un código que identifica la causa del error.

d) Rechazo (*Reject*). Indica que se ha recibido un tipo incorrecto de paquete o componente (operación rechazada). Contiene un código que identifica la causa del rechazo de la petición.

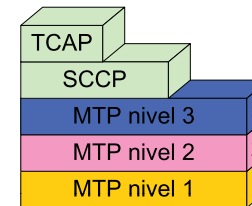


## Señalización SS7

### ▪ Transaction Capabilities Connection Part (TCAP)

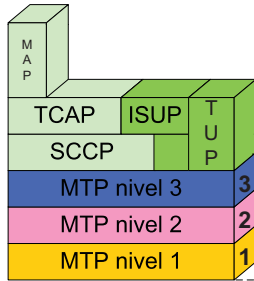
- La capa TCAP permite el desarrollo de servicios de red inteligente mediante el intercambio de información entre puntos de señalización con el servicio no orientado a conexión de SCCP.
- **Ejemplo. Red GSM.**

Cuando un cliente cambia de una nueva MSC (Mobile Switching Center), el VLR (Visitor Location Register) solicita el perfil del abonado al HLR (Home Location Register) correspondiente. Este intercambio de información se realiza mediante mensajes TCAP.



## Señalización SS7

### ▪ Mobile Application Part (MAP)

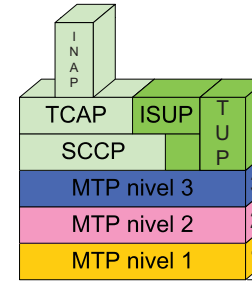


- La capa MAP es el componente más complejo de la pila SS7.
- Se utiliza en los sistemas GSM/UMTS para transferir información entre componentes de la red.
  - Localización de usuarios.
  - Autenticación
  - SMS...

Más adelante veremos ejemplos detallados de señalización MAP

## Señalización SS7

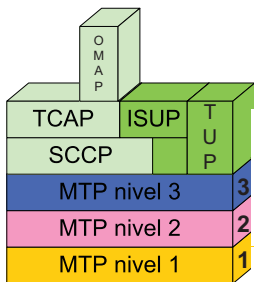
### ▪ Intelligent Network Application Part (INAP)



- La capa INAP se utiliza para implementar servicios dentro de la red, los cuales implican accesos a un SCP y pueden necesitar también acceder a periféricos inteligentes (IP).
- Los mensajes INAP se transfieren entre nodos de la red SS7 utilizando transacciones TCAP.

## Señalización SS7

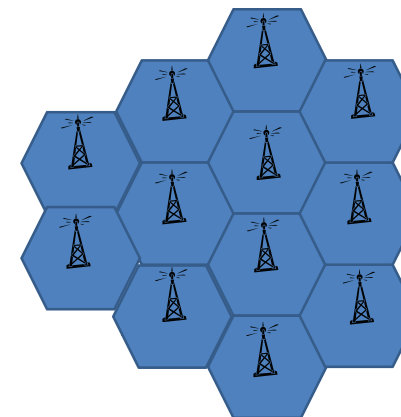
### ▪ Operations, Maintenance and Administration Part (OMAP)



- La capa OMAP se utiliza para implementar mensajes de operación, administración y mantenimiento de los nodos de la red de forma centralizada.
- La capa OMAP implementa la posibilidad de administración de bases de datos de los sistemas, configuración remota y monitorización de las prestaciones.

## Mobile Application Part (MAP)

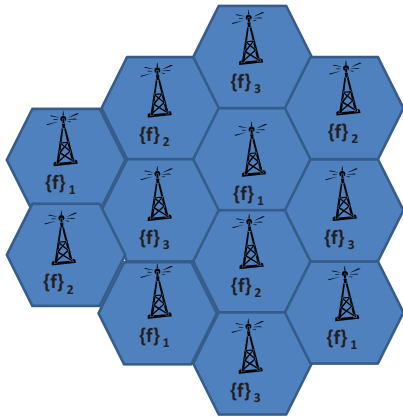
### ▪ Red Celular



¿Por qué se utiliza la estructura celular?

# Mobile Application Part (MAP)

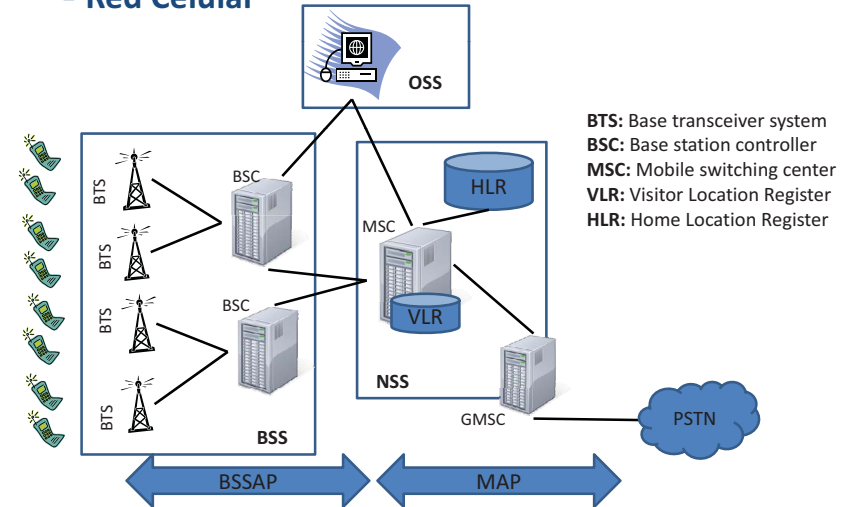
## Red Celular



- GSM/UMTS utiliza una red con estructura celular.
- Permite la re-utilización de frecuencias.
- Los terminales móviles no necesitan emitir con mucha potencia.
- Implica señalización para manejar la movilidad y los cambios de celda.

# Mobile Application Part (MAP)

## Red Celular



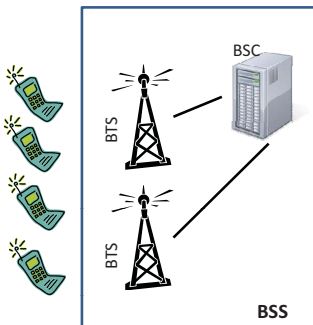
**BTS:** Base transceiver system  
**BSC:** Base station controller  
**MSC:** Mobile switching center  
**VLR:** Visitor Location Register  
**HLR:** Home Location Register

# Mobile Application Part (MAP)

## Red Celular



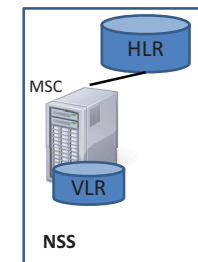
- El operation support system se emplea para la gestión de la red. Suele ser propietario.



- El Base station subsystem se encarga de la parte radio, conformando la red de acceso.
  - BTS: Transceptor radio
  - BSC: Manejo de los canales radio.
- Emplea señalización SS7, concretamente BSSAP sobre SCCP.

# Mobile Application Part (MAP)

## Red Celular



- El Network and Switching system es el encargado de la conmutación de las llamadas y contiene la inteligencia de la red para manejar la movilidad.

- Emplea el protocolo MAP sobre TCAP y SCCP.

Consta de:

- Los Mobile Switching Center realizan la conmutación de las llamadas, proveen la conexión con otras redes, y gestionan la movilidad (junto con HLR y VLR). Los Gateway MSC establecen la conexión con otras redes.
- VLR: es una base de datos local (en el área controlado por un MSC), que almacena temporalmente un subconjunto de los datos de usuario, así como su área de localización (conjunto de celdas).
- HLR: es una base de datos central (única para la red de un operador) que contiene los datos de cada usuario junto con su VLR.

*¿Cuándo hay que notificar un cambio de localización al HLR?*

## Mobile Application Part (MAP)

### ▪ Señalización en la red móvil

Algunos de los números que se emplean en la red GSM:

- IMSI – International Mobile Subscriber Identity. Identifica unívocamente al usuario y está grabado en la tarjeta SIM.
- MSISDN – Mobile Subscriber Integrated Services Digital Network Number. Es el número de teléfono al que se llama.
- MSRN – Mobile Station Routing Number. Es un número temporal que se emplea para enrutar la llamada hasta el móvil.

## Mobile Application Part (MAP)

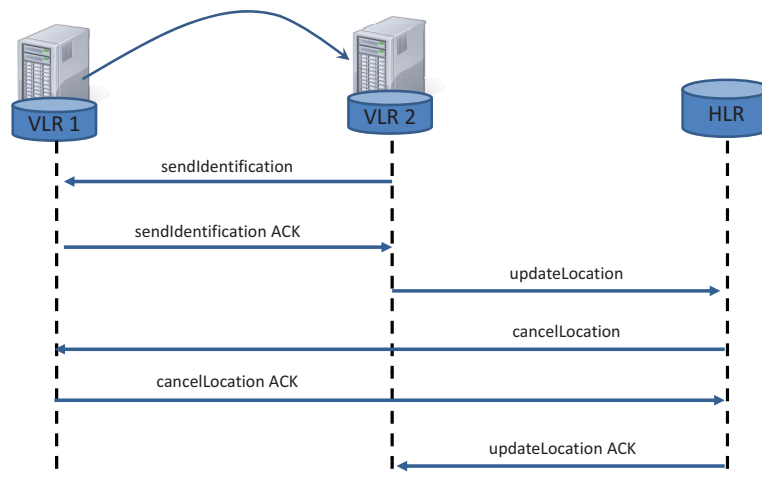
### ▪ Ejemplos de señalización en GSM

- A) Actualización de la posición de un móvil
- B) Llamada a un móvil
- C) Handover
- D) Envío de un SMS

¿Diferencia entre actualización de posición y handover?  
¿Cómo se sabe que el móvil se ha alejado de una zona?  
¿Todos los cambios de posición se señalizan por MAP?

## Mobile Application Part (MAP)

### ▪ Actualización de la posición. Mensajes MAP



## Mobile Application Part (MAP)

### ▪ Actualización de la posición. Mensajes MAP

**sendIdentification:** La nueva VLR pide los datos de identificación de usuario a la VLR antigua (esto incluye, p.e. el IMSI).

*¿Y si la antigua no tiene esa información?*

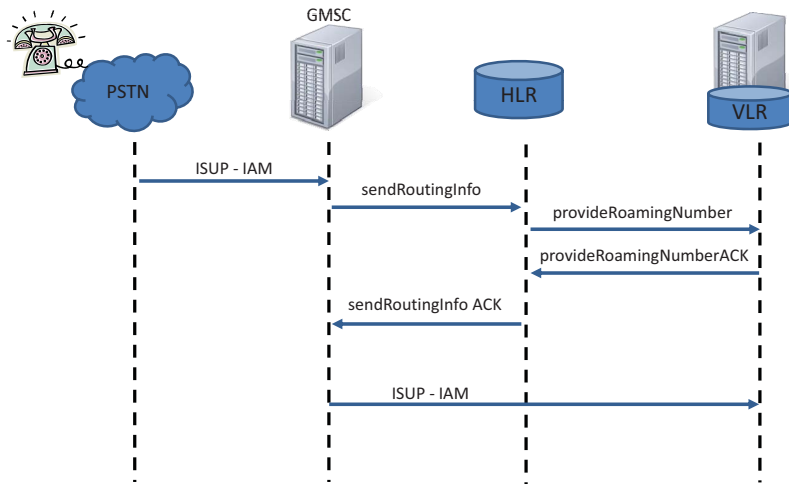
**updateLocation:** Informa a la HLR que el móvil ha realizado con éxito un cambio a un nuevo VLR, de modo que el HLR siempre conoce la posición del móvil.

**cancelLocation:** Cuando el HLR recibe un `updateLocation` desde un VLR distinto al que tiene almacenado, le dice al antiguo VLR que borre el móvil.

**updateLocation ACK:** Cuando el antiguo VLR ha borrado el móvil, se le confirma la actualización al nuevo.

## Mobile Application Part (MAP)

### ▪ Llamada a un móvil. Mensajes MAP



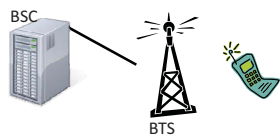
## Mobile Application Part (MAP)

### ▪ Llamada a un móvil. Mensajes MAP

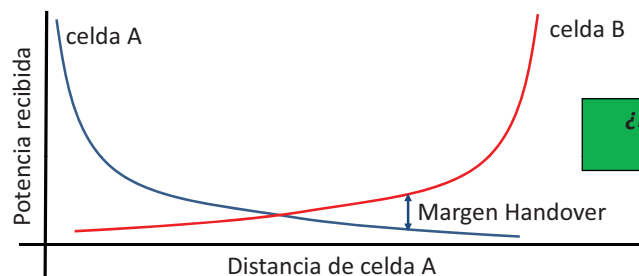
- 1) **ISUP – IAM:** El usuario marca el MSISDN del móvil y la red SS7 lleva el correspondiente mensaje ISUP hasta el GMSC.
- 2) **sendRoutingInfo:** El GMSC identifica el HLR del móvil a partir del MSISDN. Pregunta al HLR dónde se encuentra el móvil.
- 3) **provideRoamingNumber:** Gracias a las actualizaciones de posición, el HLR sabe en qué VLR está actualmente el móvil. El HLR manda el IMSI del móvil al VLR pidiendo un número de teléfono temporal para encaminar la llamada. El VLR reserva un número de teléfono temporal y lo manda al HLR.
- 4) **sendRoutingInfoACK:** El HLR manda el número temporal al GMSC.
- 5) **ISUP – IAM:** El GMSC utiliza este número para establecer la llamada usando ISUP.

## Mobile Application Part (MAP)

### ▪ Handover. Mensajes MAP

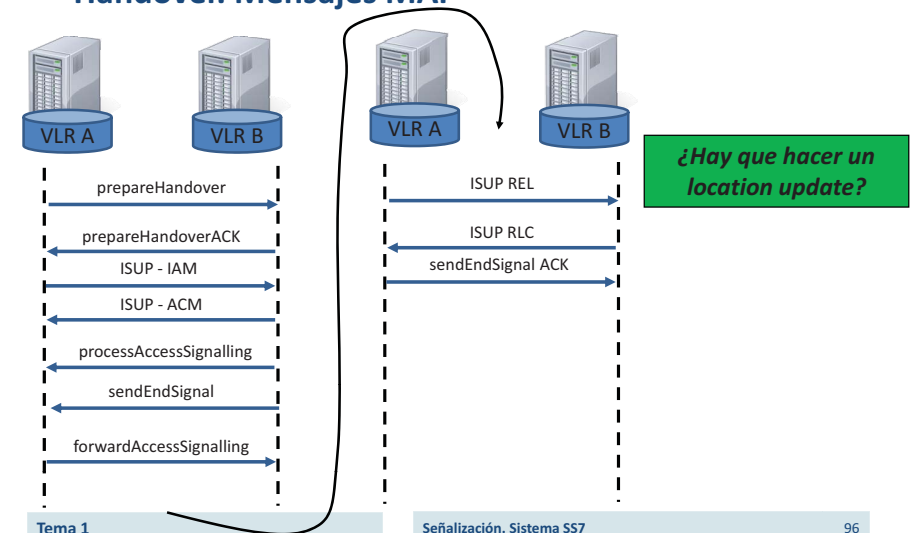


- El terminal móvil manda continuamente (cada 0.5s) a su BSC información sobre la calidad de la señal radio que recibe su celda y celdas adyacentes.
- Si es conveniente, el BSC solicita un cambio de celda, que puede implicar cambio de MSC.



## Mobile Application Part (MAP)

### ▪ Handover. Mensajes MAP



## Mobile Application Part (MAP)

### ▪ Handover. Mensajes MAP

- 1) **prepareHandover:** Solicita el Handover al MSC-B, pidiendo recursos (canal radio) para la llamada. El MSC-B contesta confirmando la reserva de recursos. El MSC-A *sigue controlando la llamada* (se le denomina MSC ancla).
- 2) **ISUP IAM / ACM:** El MSC-A establece un canal de voz con el MSC-B, y éste confirma.
- 3) **processAccessSignalling:** El terminal ha aceptado el handover. Esa información se pasa al MSC-A (ancla) en este mensaje.
- 4) **sendEndSignal:** El handover se ha completado con éxito y el MSC-A puede liberar sus recursos radio, aunque sigue controlando la llamada.
- 5) **forwardAccessSignalling:** El MSC-A (ancla) emplea este mensaje para enviar señalización al terminal móvil, a través de MSC-B.

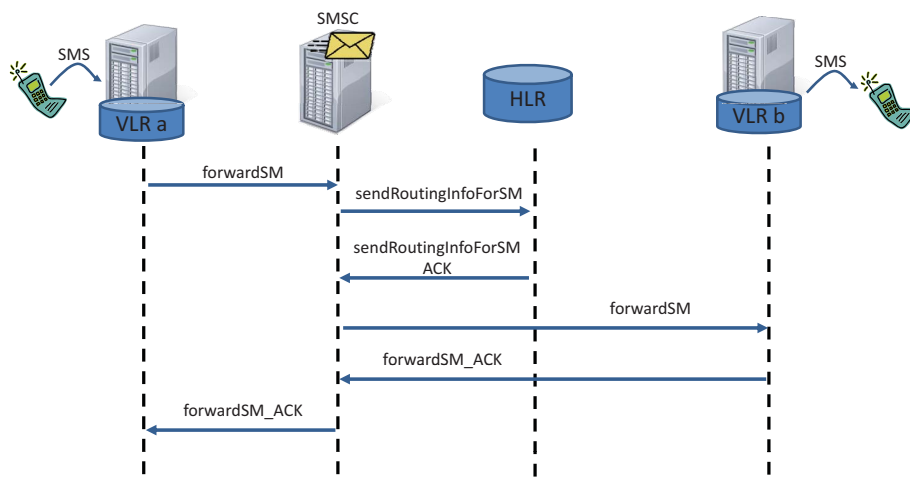
## Mobile Application Part (MAP)

### ▪ Handover. Mensajes MAP

- 6) **ISUP-REL:** Cuando el llamante cuelga, MSC-A lo notifica al MSC-B, liberando el circuito de voz entre ellos. MSC-B confirma con un ISUP-RLC.
- 7) **sendEndSignalACK:** Por el último MSC-A notifica a MSC-B que puede liberar sus recursos radio.

## Mobile Application Part (MAP)

### ▪ Envío de SMS por SS7. Mensajes MAP



## Mobile Application Part (MAP)

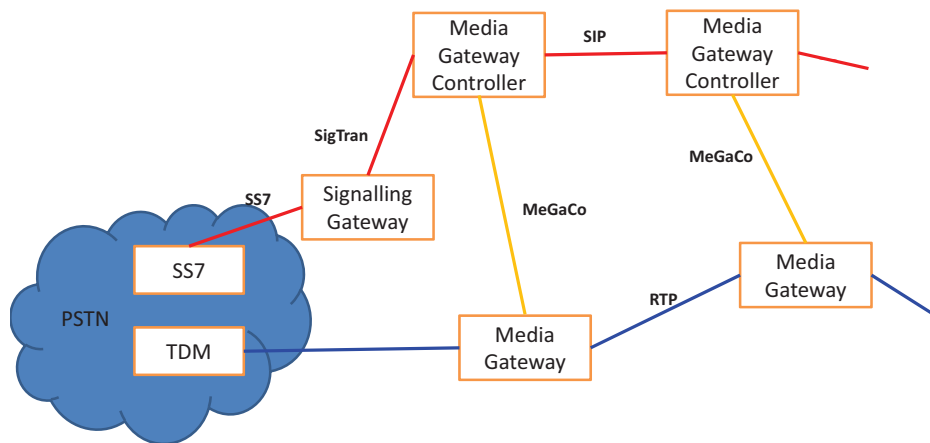
### ▪ Envío de SMS por SS7. Mensajes MAP

- 1) **forwardSM:** El contenido del SMS se manda en este mensaje MAP al centro de servicio de mensajes cortos (SMSC), que lo almacena para su re- envío. La dirección del SMSC está en la SIM.
- 2) **sendRoutingInfoForSM:** Para enviar el SMS el SMSC necesita saber dónde (en qué VLR) se encuentra. Se lo consulta a la HLR que devuelve la dirección del VLR actual.
- 3) **forwardSM:** Con la dirección obtenida del HLR el SMSC envía el mensaje al VLR. Éste confirma la entrega.



## Convergencia Voz - IP

### ▪ Signaling Transport (SIGTRAN)



## Convergencia Voz - IP

### ▪ Signaling Transport (SIGTRAN)

Para transportar voz sobre una red IP se emplean los protocolos

**RTP / RTCP (Real time protocol / Real time control protocol):** Los paquetes de voz viajan por RTP, y el nivel de calidad (paquetes perdidos, retardos, jitter...) se monitoriza con RTCP. La compresión de la voz no es responsabilidad de RTP.

**SIP (Session Initiation Protocol):** Es el protocolo de señalización empleado para establecer las sesiones (llamadas). Identifica los usuarios, encamina las llamadas, y permite a los terminales negociar los parámetros de la llamada.

¿Cómo funciona Skype?

## Convergencia Voz - IP

### ▪ Signaling Transport (SIGTRAN)

Pero, ¿cómo se integra esto con la red de telefonía convencional?

Los **Media Gateway** realizan la transcodificación de las señales PCM de la telefonía convencional y las empaquetan para su transporte mediante RTP.

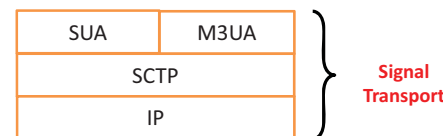
Los **Media Gateway Controllers**, que se comunican entre ellos mediante SIP, emplean el Media Gateway Control Protocol (MeGaCo) para controlar los Media Gateways.

*Nótese que esto establece la misma separación Voz/Señalización que en la red telefónica conmutada.*

La señalización SS7 de la PSTN pasa a la red IP a través de los **signalling gateways** que “traducen” SS7 a **Sigtran (Signal Transport)**.

## SIGTRAN

### ▪ Pila de protocolos en SIGTRAN

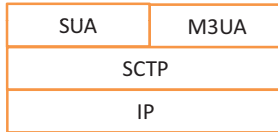


Sigtran posibilita la transmisión fiable de SS7 sobre IP.

- IP: Capa IP convencional.
- SCTP (Stream Control Transmission Protocol): Es un protocolo de transporte (como TCP) específico para señalización.
- M3UA (MTP Level 3 User Adaptation): Es una capa de adaptación (emula MTP3).
- SUA: Es una capa de adaptación que emula SCCP.

# SIGTRAN

## ▪ Pila de protocolos en SIGTRAN



¿Por qué no se usan los protocolos de transporte IP habituales, es decir, UDP y TCP?

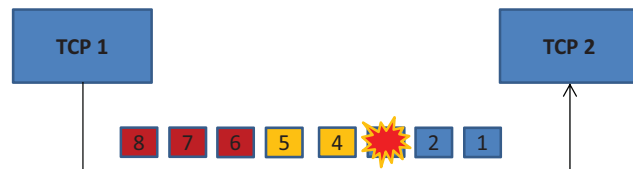
# SIGTRAN

## ▪ Pila de protocolos en SIGTRAN

- UDP no es fiable, ni entrega los paquetes en orden.
- TCP sí ofrece estas características, pero:
  - Sufre el problema de *head-of-line blocking*.
  - No detecta fallos en un enlace cuando no hay nada que transmitir (no hay *heartbeat*).
  - No permite que una conexión tenga múltiples direcciones IP (*multihoming*).

# SIGTRAN

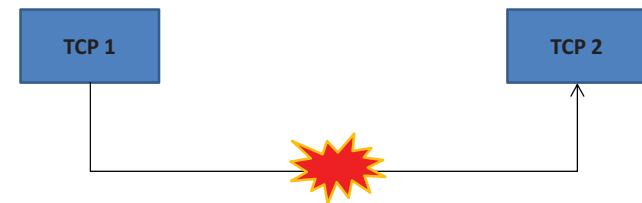
## ▪ Problemas de TCP para transporte de SS7 . Head Of Line Blocking



- Los paquetes 4, 5, ... 8 no se entregan a la capa superior (M3UA), hasta que no se haya retransmitido con éxito el paquete 3.
- Sin embargo, los paquetes 4, 5, ... 8 llevan señalización de una conexión diferente al paquete 3, por lo que realmente no haría falta esperar a entregarlos.

# SIGTRAN

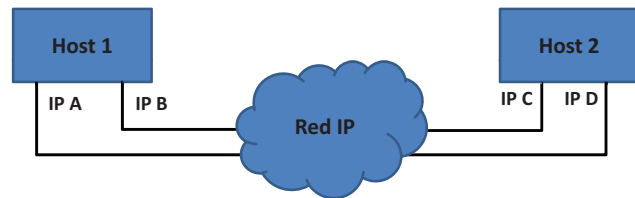
## ▪ Problemas de TCP par transporte de SS7. Heartbeat



- TCP no detecta si un enlace está roto hasta que no transmita un paquete y si de cuenta de que no recibe el ACK.

# SIGTRAN

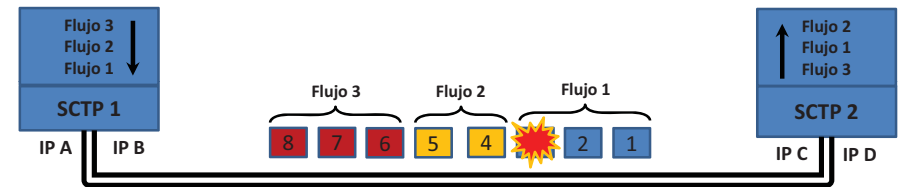
## Problemas TCP para transporte de SS7. Multihoming



- La fiabilidad / disponibilidad de la red mejora si cada host tiene dos conexiones físicas a la red, entre las que puede conmutar rápidamente si una de las conexiones falla.
- Este cambio debería ser transparente para las capas superiores.
- TCP no permite establecer una conexión sobre IPs diferentes (no soporta multihoming).

# SIGTRAN

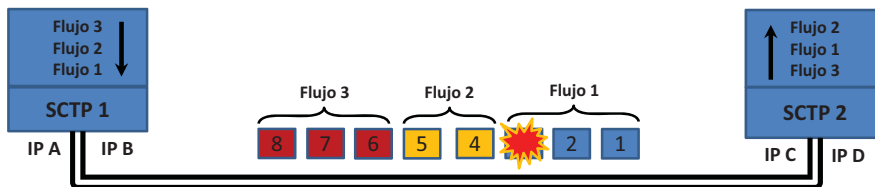
## Stream Control Transmission Protocol (SCTP)



- Permite definir flujos de paquetes: dentro de un flujo los paquetes se entregan en orden, pero un flujo puede “adelantar” a otro en la entrega a la capa superior.
- Implementa un mecanismo *heartbeat*, que sirve para comprobar el estado de la conexión aunque no se esté transmitiendo nada.
- Soporta multihoming.
- Fiabilidad parcial: Permite ponerle fecha de caducidad a un paquete. Si no se ha transmitido cuando pasa su periodo útil, se descarta.

# SIGTRAN

## Stream Control Transmission Protocol (SCTP)



¿Entonces, SCTP es mejor que TCP?

¿Y por qué no se usa también para otras aplicaciones a parte de SigTran?

Ahora la señalización se transporta con IP. ¿Qué ocurre con la seguridad?

# Análisis de la señalización

## Explotación de la red SS7

- Como se ha comentado, toda la información relativa al establecimiento, mantenimiento y liberación de las llamadas circula a través de la red de señalización.
- Además, dicha red se utiliza para enviar alarmas de los elementos de red, provocadas por fallos que pueden afectar a la calidad de los servicios ofrecidos por la operadora.
- Los sistemas de explotación de la red de señalización permite recoger las alarmas de los elementos de forma centralizada y recibir datos referentes al tráfico cursado, a partir del análisis de los mensajes transferidos por la red SS7.
- Existen dos métodos para recoger información de la red de señalización:
  - 1) Mediante ficheros enviados por los puntos de señalización
  - 2) Mediante sondas

# Análisis de la señalización

## ▪ Explotación de la red SS7

- Suele ser más interesante la recogida de datos mediante sondas, dado que son independientes del fabricante.
- Dichas sondas poseen un hardware dedicado para la monitorización de enlaces SS7 y se ubican en puntos específicos de la red.
- Entre las aplicaciones más importantes, destacan:
  - Generación de CDR (Call Detail Record) /TDR (Transactional Detail Record) en tiempo real
  - Análisis de tráfico y eficiencia de la red
  - Análisis de protocolo
  - Trazado de llamadas

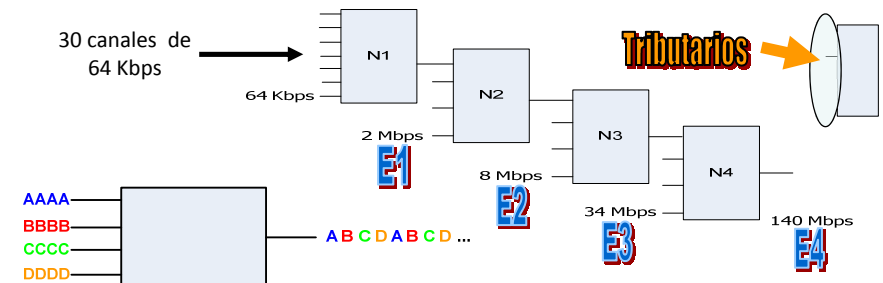
## Tema 2. Redes Síncronas - SDH

### ▪ Índice

- 2.1 Introducción a PDH
- 2.2 Introducción a SDH
- 2.3 Arquitectura SDH
- 2.4 Tramas SDH
- 2.5 Multiplexación
- 2.6 Taras en SDH
- 2.7 Sincronización
- 2.8 Protección contra fallos
- 2.9 Diferencias SONET/SDH
- 2.10 ¿Qué viene después de SDH?

## 1. Introducción a PDH

- PDH (Jerarquía Digital Plesiócrona) es el antecesor de SDH (Jerarquía digital síncrona)
- PDH estaba diseñado para la multiplexación de tráfico telefónico mediante multiplexación por división en tiempo.
- Jerarquía europea:



## 1. Introducción a PDH

### ▪ Inconvenientes de PDH

- Jerarquías diferentes en Europa, EE.UU. y Japón: problemas de interconexión.
- Resulta complicado localizar un canal dentro de una trama ya que:
  - En PDH se realiza una multiplexación mediante el entrelazado bit a bit.
  - Al ser plesiócrono (casi-síncrono), cada nodo tiene su propio reloj y hace falta usar bits de relleno
  - En consecuencia, para extraer un canal de un nivel de multiplexación alto hay que **demultiplexar todos los canales**.
- Poca capacidad de señalización, lo que complica la gestión de la red.
- No están estandarizados:
  - las velocidades superiores a 140Mbps.
  - el nivel físico (cable de cobre).
  - la gestión de la red.

## 1. Introducción a SDH

### ▪ Evolución a SDH

La fibra óptica desplaza al cobre como medio de transmisión.

En los años 80 se desarrolla en EE.UU. el estándar SONET y, a partir de él, la ITU estandariza SDH (ITU-T G.78x). El estándar SDH abarca:

- Definición de una jerarquía estructurada de multiplexación.
- Definición de las técnicas de gestión de red y protección frente a enlaces rotos.
- Definición de una capa física y una interfaz con la misma estandarizada (fibra óptica o enlaces radio).
- Definición de las interfaces con otros protocolos, sobre SDH.

SDH es el estándar de transmisión que se emplea actualmente en la mayoría de las redes de transporte.

## 2. Introducción a SDH

### ▪ De PDH a SDH

La fibra óptica desplaza al cobre como medio de transmisión.

En los años 80 se desarrolla en EE.UU. el estándar SONET y, a partir de él, la ITU estandariza SDH (ITU-T G.78x). El estándar SDH abarca:

- Definición de una jerarquía estructurada de multiplexación.
- Definición de las técnicas de gestión de red y protección frente a enlaces rotos.
- Definición de una capa física y una interfaz con la misma estandarizada (fibra óptica o enlaces radio).
- Definición de las interfaces con otros protocolos, sobre SDH.

SDH es el estándar de transmisión que se emplea actualmente en la mayoría de las redes de transporte.

## 2. Introducción a SDH

### ▪ Ventajas de SDH

- **Permite altas tasas de transferencia.** Con la tecnología SDH es posible disponer de tasas de transferencia de 155Mbit/s hasta 40 Gbit/s. Esto hace de la tecnología SDH la más apropiada para redes backbone. Las altas velocidades son consiguen con transmisión por fibra óptica.
- **Función insertar/extraer (add/drop) simplificada.** Al ser una red completamente síncrona es mucho más fácil extraer o insertar canales de baja tasa de transferencia en flujos de alta tasa de transferencia que en las redes PDH. Para ello no es necesario demultiplexar y multiplexar como ocurría en las redes plesiócronicas.
- **Alta disponibilidad y escalabilidad.** Lo que permite a los proveedores reaccionar rápidamente ante los requisitos de los usuarios (menor tiempo de indisponibilidad y mayor ancho de banda). Esto es en parte consecuencia de las facilidades para la gestión y monitorización de la red (Telecommunications Management Network).

## 2. Introducción a SDH

### ▪ Ventajas de PDH

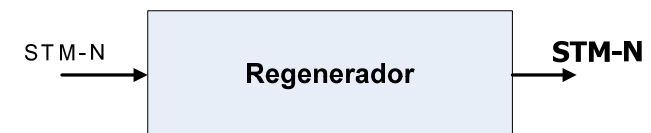
- **Alta fiabilidad.** Las redes SDH disponen de mecanismos que proporcionan cierta tolerancia a fallos, pudiendo recuperarse automáticamente de fallos en el sistema o de la rotura de enlaces.
- **Apropiada para nuevos servicios.** Esta tecnología resulta apropiada para los actuales servicios demandados por los usuarios como WAN, LAN, difusión de video bajo demanda, VoIP, etc. Además, es la tecnología actualmente utilizada con protocolos como ATM. Para el transporte de diferentes tipos de tráfico emplea SDH define **contenedores virtuales (VC)**.
- **Interconexión.** La tecnología estandarizada hace mucho más fácil la interconexión con otros operadores a nivel mundial. Además, existen diferentes suministradores para los equipos de red, con la consiguiente reducción en el coste de los mismos.

## 3. Arquitectura de red SDH

### ▪ Componentes

- Las tramas SDH se denominan **módulos de transporte síncrono (STM - Synchronous Transport Module)**. STM-1 es la trama base y su velocidad es de 155.52 Mbps.
- Actualmente, las redes SDH se componen de **cuatro** tipos básicos de **elementos de red**. La topología de red (usualmente, en anillo o en malla) la decide la operadora de red.

- 1) Regeneradores.** Su función consiste en regenerar la señal de reloj y la amplitud de la señal de entrada, la cual ha podido sufrir atenuaciones o distorsiones. La señal de reloj se extrae del flujo de datos de entrada.



### 3. Arquitectura de red SDH

#### Componentes

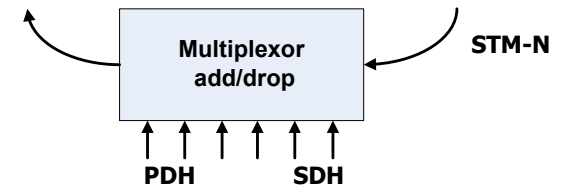
- 2) **Multiplexores terminales.** Su función consiste en combinar señales de entrada síncronas o plesiócronas para obtener un nuevo flujo de datos de una tasa mayor (señales STM-N).



### 3. Arquitectura de red SDH

#### Componentes

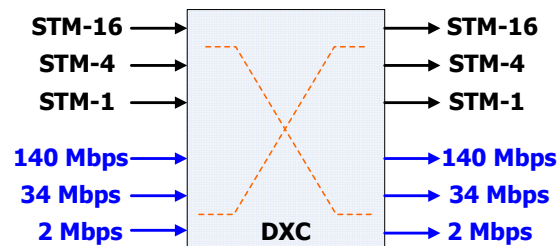
- 3) **Multiplexores add/drop (ADM).** Su función es permitir la inserción o extracción de señales síncronas de baja tasa así como señales plesiócronas en tramas SDH. Gracias a los multiplexores add/drop es posible mantener una topología en anillo, que como se verá más adelante, permite la conmutación automática a enlaces de respaldo en el caso de un fallo en un enlace o en un elemento de la red.



### 3. Arquitectura de red SDH

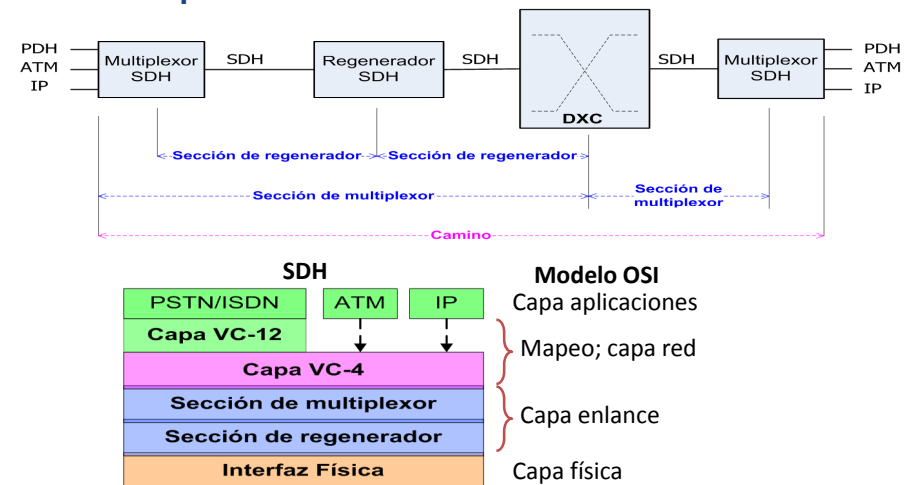
#### Componentes

- 4) **Digital cross-connect (DXC).** Este elemento realiza diferentes funciones. Permite el mapeo de señales tributarias PDH en contenedores virtuales SDH, así como la conmutación de contenedores virtuales.



### 3. Arquitectura de red

#### Pila de protocolos



### 3. Arquitectura de red

#### ▪ Pila de protocolos

##### Capa de Camino / VC

- Establecimiento de las conexiones extremo a extremo.
- Control del estado de las conexiones. Mantenimiento de las conexiones.

##### Sección de regenerador

- Define las operaciones llevadas a cabo por los regeneradores y entre regeneradores.

##### Sección de multiplexor

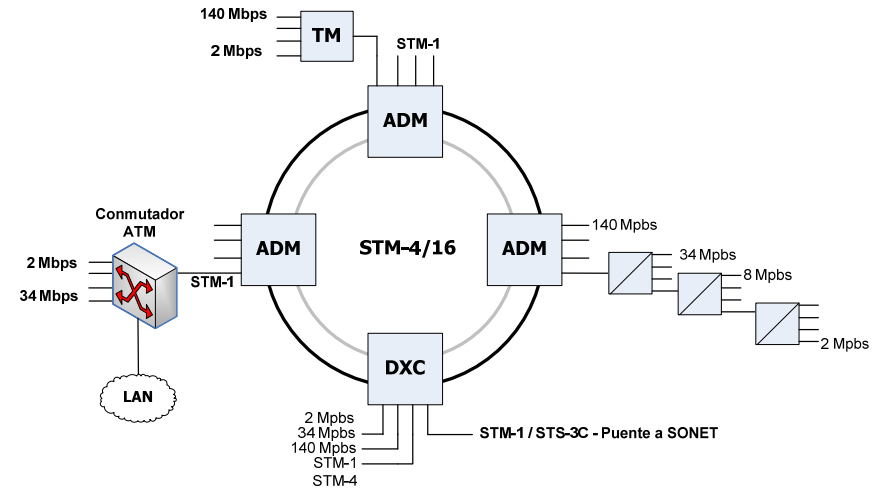
- Multiplexación de las conexiones entre dos nodos
- Protección y recuperación frente a enlaces rotos

##### Interfaz física

- Define las señales necesarias para la transmisión a través del medio físico (fibra óptica o enlace radio).

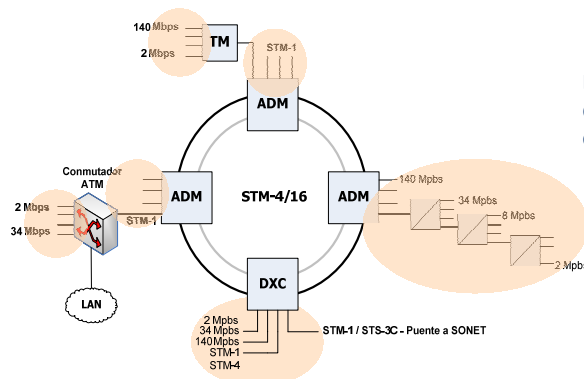
### 3. Arquitectura de red

#### ▪ Topología de red



### 3. Arquitectura de red

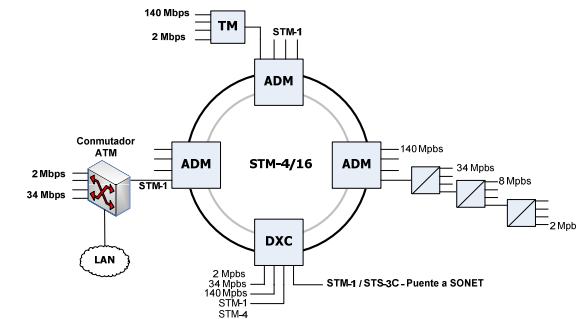
#### ▪ Tributarios



En la Figura se muestra un diagrama típico de un anillo SDH con varios tributarios.

### 3. Arquitectura de red

#### ▪ Tributarios



Como puede verse en la figura, se mezclan diferentes aplicaciones. Esto es típico de SDH, la cual, debe ser capaz de transmitir señales plesiócronas a la vez que protocolos como ATM.

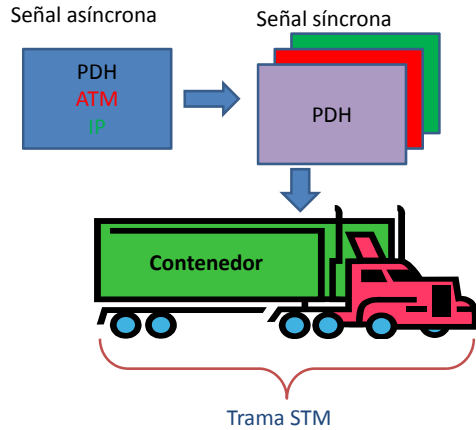
Para que esto sea posible, es necesario utilizar los diferentes elementos de una red SDH (multiplexores, Cross-Connect DXC, etc.).



## 4. Tramas en SDH

### Contenedores

Los tributarios se introducen en un **contenedor**. Hay un contenedor diferente para cada velocidad.

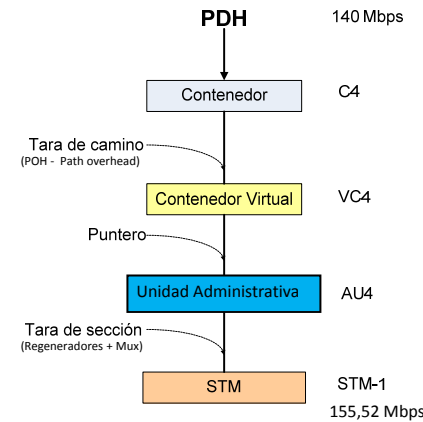


Tipos de contenedores

Conten.	Tasa binaria
C-11	1,6 Mbps
C-12	2,176 Mbps
C-2	6,784 Mbps
C-3	48,384 Mbps
C-4	149,76 Mbps

## 4. Tramas en SDH

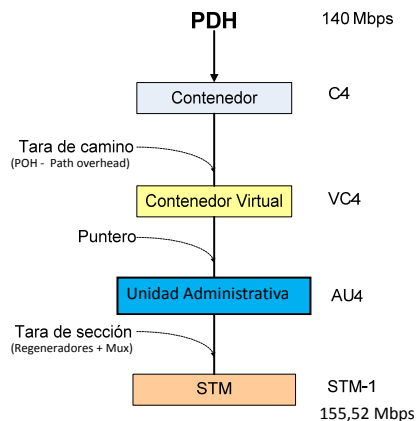
### Formación de la señal síncrona a partir de PDH



- El **contenedor** es la unidad básica para los canales **tributarios**.
- En el caso de canales PDH, se utilizan contenedores C-n cuyo tamaño es mayor que la **carga útil** (payload) a transmitir.
- La capacidad restante se utiliza parcialmente para la **justificación** (*stuffing*) de forma que sea posible corregir **desfases temporales** en las señales PDH.
- El **contenedor virtual** se forma añadiendo la tara de camino a un contenedor. Un CV no se modifica durante la tx por la red.

## 4. Tramas en SDH

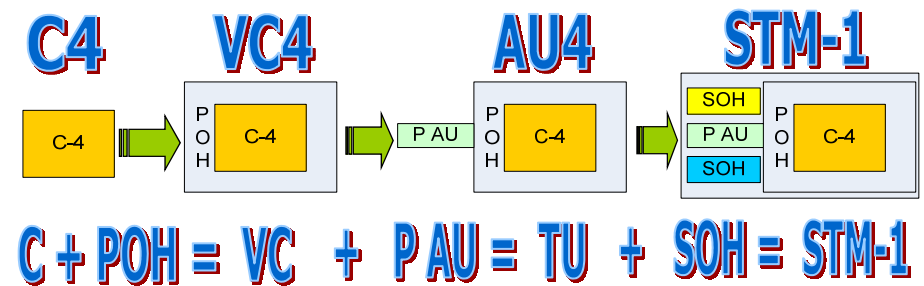
### Formación de la señal síncrona a partir de PDH



- El puntero indica dónde empieza el contenedor virtual dentro de la carga útil.
- Se llama **unidad administrativa** al contenedor virtual más el puntero.
- Tara sección = Tara regenerador + Tara multiplexador
- Un módulo de transporte se forma a partir de una unidad administrativa y la tara de sección (tanto de regeneradores como de multiplexores).

## 4. Tramas en SDH

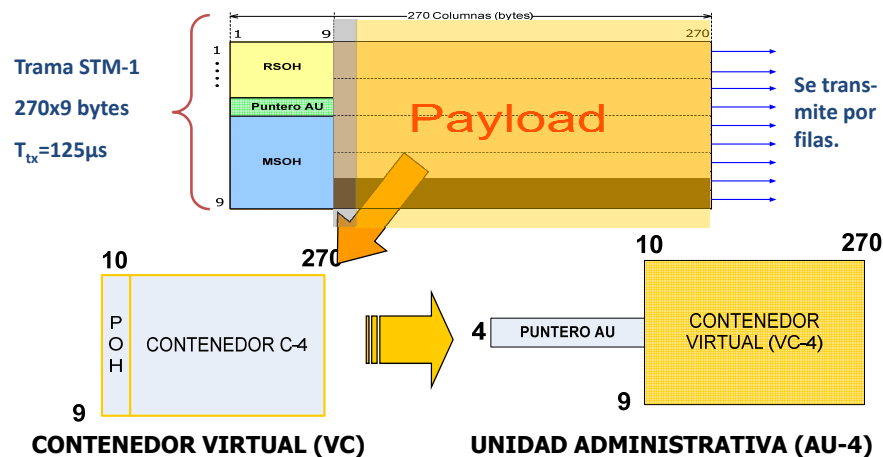
### Formación de la señal síncrona STM



$$C + POH = VC + PAU = TU + SOH = STM-1$$

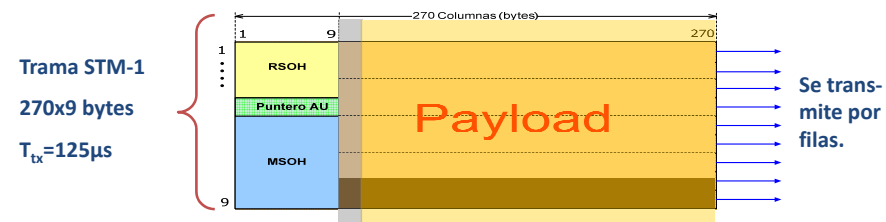
## 4. Tramas en SDH

### Formato de la trama STM



## 4. Tramas en SDH

### Formato de la trama STM



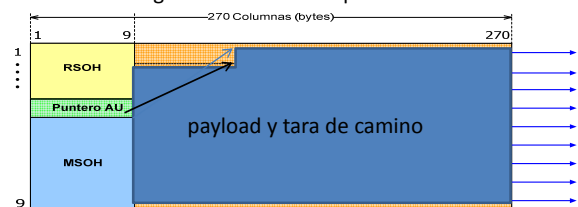
Calcular, para una trama STM-1, los siguientes regímenes binarios:

- Uno de los canales de 1 byte. ¿Por qué tiene esa velocidad?
- La trama completa.
- La carga útil, y la carga útil menos la tara de camino (suponiendo que es una columna).
- La tara de sección de regenerador.

## 4. Tramas en SDH

### Formato de la trama STM

- La información transportada es, generalmente, asíncrona. Ej: Canal PDH de 140Mbps.
- Pero las tramas STM-1 son completamente síncronas.
- La velocidad de la carga útil (Payload) menos la tara de camino son  
 $(270-9-1) \text{ columnas} \times 9 \text{ filas} \times 8\text{bits} / 125\mu s = 149,76\text{Mbps}$
- El espacio sobrante se emplea para insertar la información en el momento que ésta llegue. Los bytes no ocupados se rellenan. **El VC puede "flotar" entre dos STMs consecutivos!**
- El puntero indica el principio de la tara de camino. Así resulta sencillo de demultiplexar y no son necesario búferes grandes en los multiplexores.



## 4. Tramas en SDH

### Justificación. Punteros

RSOH						522															
						Justificación positiva										782					
H1	%	%	H2	%	%	H3	H3	H3	0				1	.....	86						
MSOH						87							88	.....	173						
						Justificación negativa														.....	
														521							

- Los 261x9 = 2349 bytes del VC se numeran de tres en tres (0 a 782).
- Los bytes H1 y H2 juntos contienen el valor del puntero (0 a 782).

## 4. Tramas en SDH

### Justificación. Punteros

La justificación compensa pequeñas diferencias de velocidad entre tramas síncronas.

Cuando el flujo de entrada es más lento que la STM-1:

- Llega un momento en que cuando se va a transmitir la siguiente trama STM-1 aún no han llegado los datos. Entonces:
- Cambiando algunos bits de H1, H2 se avisa de que se va a hacer justificación positiva. El receptor sabe entonces que debe ignorar los 3 bytes que siguen al último byte H3.
- Se inserta el VC en una posición tres bytes más alta (más tarde), y el puntero se incrementa en 1.

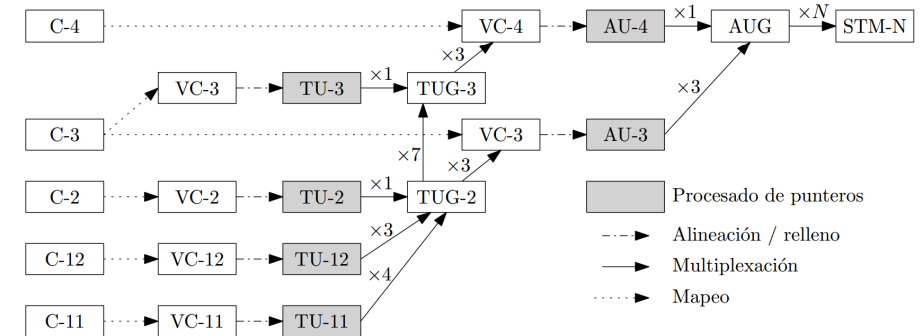
Cuando el flujo de entrada es más rápido que la STM-1:

- Llega un momento en que sobra información. Entonces:
- Con algunos bits de H1, H2 se avisa de justificación negativa. El receptor entonces sabe que debe leer los tres bytes H3 (que normalmente ignora).
- Se inserta el VC en un posición tres bytes más baja (llega antes), y puntero se decrementa en 1.

## 5. Multiplexación

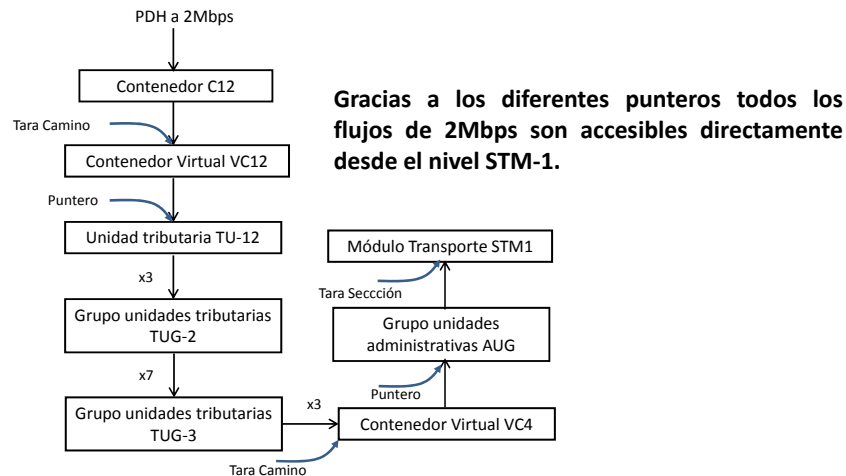
### Jerarquía SDH

- Cuando se transmiten flujos más lentos (p.e. PDH a 2 Mbps), éstos se agrupan.
- Cuando se forman grupos, **no** se añaden bits.
- Las unidades tributarias son unidades administrativas de un nivel de multiplexación más bajo, y están compuestas por contenedor virtual + puntero.



## 5. Multiplexación

### Jerarquía SDH

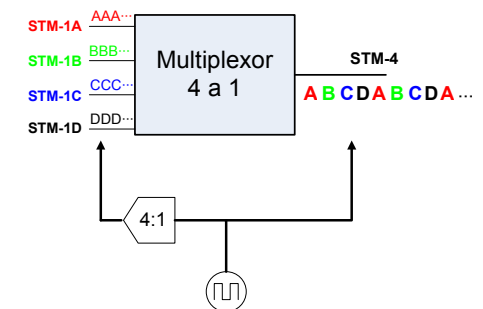


Gracias a los diferentes punteros todos los flujos de 2Mbps son accesibles directamente desde el nivel STM-1.

## 5. Multiplexación

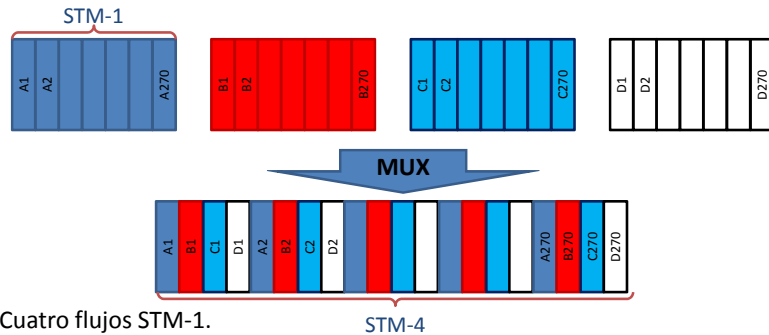
### Multiplexación tramas STM

- Las señales STM-1 pueden multiplexarse para dar lugar a señales STM-N de tasa más alta.
- Dicha multiplexación se realiza de forma síncrona en el nodo.
- En el caso de la generación de una señal STM-4, el reloj de transmisión hacia la línea de salida tiene una frecuencia 4 veces superior a la de los procesos STM-1 síncronos.
- En SDH, todo el procesamiento de tributarios se realiza a nivel de tramas STM-1.



## 5. Multiplexación

### ▪ Multiplexación tramas STM



- Cuatro flujos STM-1.
- 4x9 columnas de tara y 4x261 columnas de carga útil.
- Se sigue transmitiendo por filas; toda la trama STM-N se tx en 125µs.
- Están definidas: STM-1, STM-4, STM-16, STM-64 y STM-256

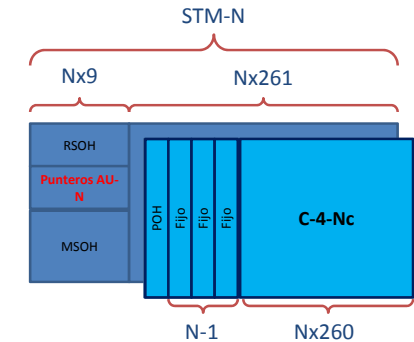
¿ Cual es el régimen binario de una trama STM-N ?

## 5. Multiplexación

### ▪ Concatenación

¿ Es posible transmitir un único flujo de más de 155.52 Mbps ?

- El contenedor concatenado (C-4-Nc) no está subdividido.
- Se puede rellenar byte a byte, por ejemplo con celdas ATM.
- El primer puntero AU indica el POH.
- Los demás están puestos a un valor especial que indica la concatenación.

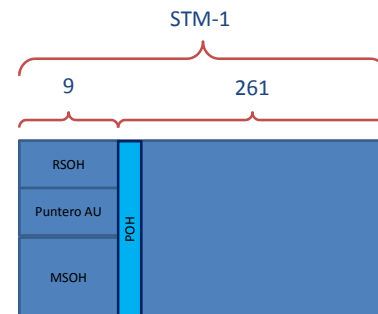


## 6. Overhead en SDH (Taras)

### ▪ Taras de Sección y de camino

Las taras, también llamadas *overhead* son carga no útil contenida en las tramas y que transportan información de señalización o control.

- **Tara de Sección (Section Overhead):** Los nueve primeros bytes de cada una de las 9 filas, y se componen de:
  - Tara de sección de regenerador (3 filas).
  - Tara de sección de multiplexor (5 filas).
- **Tara de camino (Path Overhead):** Está dentro del VC.



## 6. Overhead en SDH (Taras)

### ▪ Taras de Sección y de Multiplexor

A1	A1	A1	A2	A2	A2	J0			Tara regenerador
B1			E1			F1			
D1			D2			D3			
Puntero AU									
B2	B2	B2	K1			K2			Tara multiplexor
D4			D5			D6			
D7			D8			D9			
D10			D11			D12			
S1					M1	E2			

Reservado red  
Dependiente del medio físico

## 6. Overhead en SDH (Taras)

### ▪ Taras de Sección y de Multiplexor

- **A1, A2** Alineamiento de trama: indican el comienzo de la trama.
- **B1, B2** Monitorización de calidad a nivel de regenerador y multiplexor. Bytes de paridad calculados sobre la trama STM-N anterior.
- **D1..D3** Proporcionan un canal para gestión y mantenimiento de 192kbps.
- **D4..D12** Proporcionan un canal para gestión y mantenimiento de 576kbps.
- **E1, E2** Conexiones de voz para operarios de la red.
- **F1** Reservado para el usuario (operador de la red).
- **J0** Identificador de traza: Sirve para que el receptor compruebe que sigue conectado con el transmisor.
- **K1, K2** Control APS (Automatic protection switching). Se usan para indicar fallos en la red y intentar solventarlos.
- **S1** Indicador calidad reloj, utilizando el protocolo synchronization status messaging (SSM).
- **M1** Reconocimiento de error de transmisión. Indica cuántos errores se han detectado con los bytes de paridad B2.

## 6. Overhead en SDH (Taras)

### ▪ Taras de Camino

La tara de camino (POH) junto con un contenedor forman un contenedor virtual (VC). La tara de camino incluye información de monitorización de la calidad del enlace e indica el tipo de contenedor. Por tanto, el formato y el tamaño de la tara de camino depende del tipo de contenedor:

- Tara de camino VC-3 y VC-4
- Tara de camino VC11 y VC-12

## 6. Overhead en SDH (Taras)

### ▪ Taras de Camino

<b>J1</b>	Identificador de camino: Sirve para que el receptor compruebe que sigue conectado con el transmisor.
<b>B3</b>	Monitorización de calidad a nivel de regenerador y multiplexor. Byte de paridad calculados sobre el contenedor virtual de la trama anterior.
<b>C2</b>	Índica el tipo de contenedor y la info transportada (así se sabe cómo demux).
<b>G1</b>	Manda información de errores de transmisión de vuelta al transmisor.
<b>F2</b>	Reservado para el usuario.
<b>H4</b>	Indicador de supertrama.
<b>F3</b>	Reservado para el usuario.
<b>K3</b>	Señalización de APS (Automatic Protection Switching).
<b>N1</b>	Para control de errores cuando se atraviesan redes de diferentes operadores (Tandem Connection Monitoring)

## 6. Overhead en SDH (Taras)

### ▪ Taras de Camino

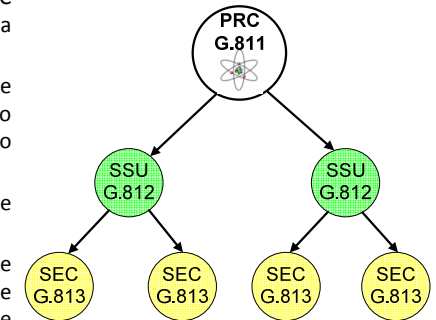
<b>V5</b>	Indicación y monitorización de error.
<b>J2</b>	Indicador de camino. Sirve para que el receptor compruebe que sigue conectado con el transmisor.
<b>N2</b>	Para Tandem Monitoring
<b>K4</b>	Para APS (Automatic Protection Switching).

## 7. Sincronización

- La sincronización en SDH es especialmente importante, pues se quiere que, como su propio nombre indica, que sea una tecnología realmente síncrona. El hecho de ser una red síncrona, la hace mucho menos tolerante a desfases entre los relojes de los diferentes nodos de la red, degradándose rápidamente el rendimiento y pudiendo provocar incluso la caída de la red.
- Para evitar esto, en SDH todos los nodos de la red se sincronizan con un reloj de referencia (Reloj de referencia primario o PRC) de alta precisión.
- Dicho reloj se distribuye por la red siguiendo las estructuras jerárquicas descritas, a través de los mismos circuitos SDH.

## 7. Sincronización

- La señal de sincronización se regenera en las SSU (Synchronization Supply Units) y en los SEC (Synchronous equipment Clock), con la ayuda de bucles enganchados en fase (PLL).
- En el caso de que deje de recibirse la señal de reloj primario en un nodo, dicho nodo conmuta a otra fuente de reloj de igual o menor calidad que la fuente primaria.
- Si no fuese posible conmutar a otra fuente de reloj, el nodo pasa a modo "holdover".
- En este modo, la señal de reloj se mantiene relativamente precisa utilizando los valores de corrección de frecuencia almacenados, y que han sido utilizados en las últimas horas.



## 7. Sincronización

- Es esencial evitar las "islas de reloj" que se comportan como relojes libres (*free-running*) y que con el paso del tiempo, podrían provocar la pérdida de sincronismo y el fallo total de la red.
- Para evitar las "islas de reloj" se envía señalización entre los elementos de red que contiene información sobre el estado de la sincronización, a través de los mensajes SSM. El SSM informa al elemento vecino sobre el estado de la fuente de reloj, y es parte de la cabecera de la sección de multiplexación (byte S1).
- Con la interconexión de redes que poseen fuentes de reloj primarias independientes, pueden aparecer problemas de sincronismo que puede solucionarse con los punteros hasta cierto punto. Si la red presenta muchos ajustes de puntero, puede indicar un problema de sincronismo.

## 8. Protección contra fallos

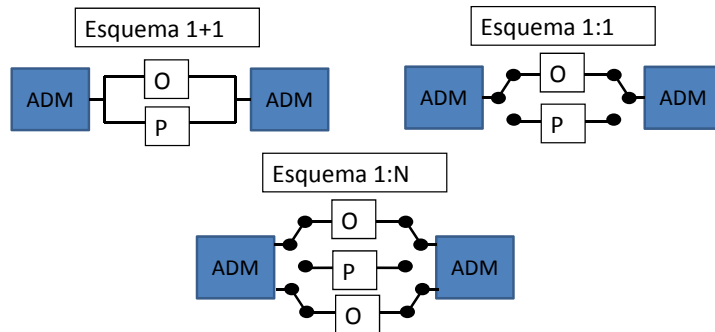
- SDH debe ser muy fiable (funcionar el 99,999% del tiempo).
- Debe recuperarse muy rápidamente de un error (< 50ms).
- SDH dispone de un mecanismo de protección que entra en funcionamiento en caso de un fallo en un nodo o en un enlace.
- En caso de fallo en un enlace, dicho enlace es redirigido a un circuito de respaldo (back-up).
- Este mecanismo de protección se denomina APS (Automatic Protection Switching).
- La función APS está controlada utilizando los bytes K1 y K2 de la cabecera.

## 8. Protección contra fallos

### ■ Esquemas de protección lineales

Se distingue protección en enlaces **lineales** y **anillos**. Ambos se basan en enlaces redundantes: **fibra operativa (O)** + **fibra de protección (P)**.

Los esquemas de protección en un **enlace lineal** son:

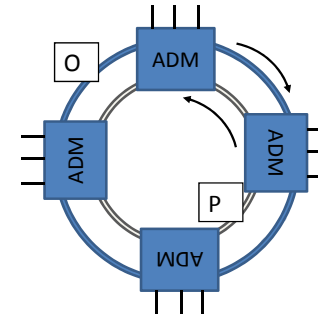


## 8. Protección contra fallos

### ■ Esquemas de protección en anillos

Los esquemas de protección para un **anillo SDH** más comunes son:

- Protección de la conexión de subred (SubNetworkConnectionProtection)
- Anillo de protección en sección de multiplexor con dos fibras (MultiplexSection-SharedProtectionRing)
- Anillo de protección en sección de multiplexor con cuatro fibras

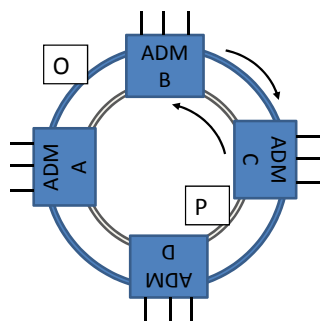


Vamos a ver los primeros dos.

- Hay dos anillos de fibra: working y protection.
- La transmisión por cada anillo es siempre en una sola dirección.
- La dirección de transmisión es opuesta en los dos anillos.

## 8. Protección contra fallos

### ■ Protección de la conexión de subred (SNCP)

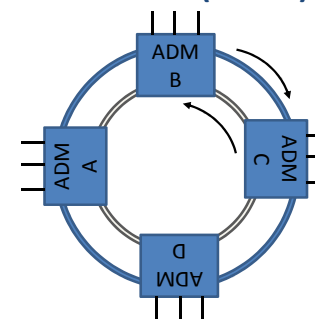


Suponemos que se transmite información de A a B. El esquema es parecido al 1+1 lineal.

- La info se transmite tanto por la fibra operativa (A → B) como por la de protección (A → D → C → B)
- B elige la señal con mayor calidad.
- Ventaja: simple de implementar.
- Desventaja: Misma capacidad de transmisión que con una fibra (caro).
- En condiciones normales B tx a A por la ruta B → C → D → A

## 8. Protección contra fallos

### ■ Anillo de protección en sección de multiplexor con dos fibras (MSPR)



- Ambas fibras usan la mitad de su capacidad para tráfico operativo y la otra para tráfico de protección.
- El envío de información es bidireccional eligiéndose la ruta más corta (A tx a B por el anillo exterior y B a A por el interior).
- Si no hay fallo la capacidad de protección puede usarse para tráfico de baja prioridad.
- Supongamos que A transmite a C siguiendo la ruta A → B → C, y falla en enlace entre A y B.
- Al ser la protección a nivel de multiplexor, la protección busca un nuevo camino al salto siguiente, de donde el tráfico sigue su curso normal. A → D → C → B → C.

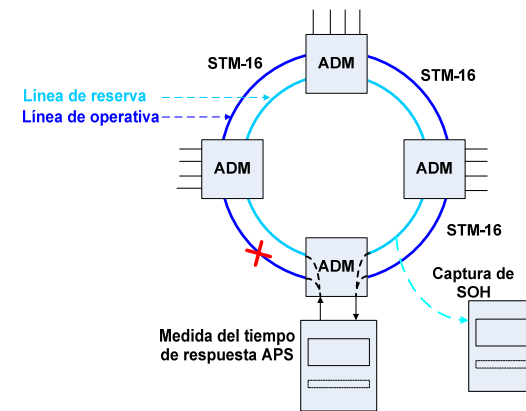
## 8. Protección contra fallos

### ▪ Fallo en un nodo

¿Qué ocurre en ambos esquemas (SNCP y MS-SPR) cuando falla un nodo?

## 8. Protección contra fallos

### ▪ Medida de prestaciones



- Para comprobar que la conmutación a la línea de reserva se realiza en menos de 50ms, existen equipos que miden el tiempo de respuesta (ej. pérdida de un patrón de prueba).
- Un retardo excesivo en la conmutación degrada las prestaciones de la red y puede llegar a provocar un fallo total.

## 9. SONET y SDH

### ▪ Diferencias

- SDH es la jerarquía digital síncrona utilizada en todo el mundo excepto en EEUU, Canadá y Japón. En dichos países, el estándar equivalente a SDH recibe el nombre de SONET.
- La tasa de transferencia proporcionada por SONET es de 51.84 Mbps y la trama que transporta la información (equivalente a la STM-1 de SDH) se denomina STS-1 (Synchronous Transport Signal).
- Si el medio físico es fibra óptica, la señal (equivalente a un contenedor C-1 en SDH) se denomina OC-1 (Optical Carrier).
- De la misma forma que en SDH, en SONET existen diferentes niveles de jerarquía, para proporcionar tasas de transferencia desde 51.84 Mbps (STS-1) hasta 9953.28 Mbps (STS-192)
- **Las cosas funcionan igual pero se llaman de distinta forma**

## 10. ¿Qué viene después de SDH?

### ▪ Tecnología de futuro: OTH?

- OTH es un estándar nuevo pensado para sustituir SDH.
- La principales mejoras respecto a SDH son:
  - Uso de FEC (Forward error correction): Códigos para corregir errores, no sólo detectarlos. Permite trabajar con potencias más bajas, lo que se traduce en tramos de fibra más largos y/o con más elementos.
  - Más nivel de Tandem Connection Monitoring.
  - Transporta de manera transparente señales SDH.
  - Conmutación de velocidades más altas. SDH conmuta (procesa tramas) a velocidad de STM-1, pero ya soporta flujos de 40Gbps, lo que supone conmutar 256 veces. OTH permite conmutar flujos de cualquier velocidad.



## Tema 3. Redes Asíncronas - ATM

### ▪ Índice

- 3.1. Introducción. Redes de banda ancha
- 3.2. Modo de Transferencia Asíncrono
- 3.3. Transparencia en la transmisión
- 3.4. Celdas ATM
- 3.5. Conexiones virtuales
- 3.6. Control de errores
- 3.7. Delineación de celda
- 3.8. Modelo de referencia
- 3.10. Gestión del tráfico
- 3.11. Señalización en ATM

## 1. Introducción. Redes de banda ancha

### ▪ Introducción

- La tendencia hacia los servicios multimedia que combinan sonido, imágenes y texto a la vez que video, así como aplicaciones de tiempo real, han revolucionado las redes en la última década, planteando nuevos desafíos a las operadoras.
- Por otro lado, existe una red telefónica capaz de transmitir voz y datos de banda estrecha.
- Con el objeto de disponer de una red unificada, que pudiese ser utilizada para diferentes servicios y aplicaciones, actuales y futuras, independientemente de los requisitos de ancho de banda, surgió la RDSI (*Red Digital de Servicios Integrados*).
- La idea de una red de digital de servicios integrados está detrás de ATM (Modo de transferencia asíncrono).

## 1. Introducción. Redes de banda ancha

### ▪ Introducción

- De hecho, la tecnología ATM juega un papel muy importante en las redes de *backbone*, que tienen que transportar datos de diferentes aplicaciones actuales como video bajo demanda o VoIP.

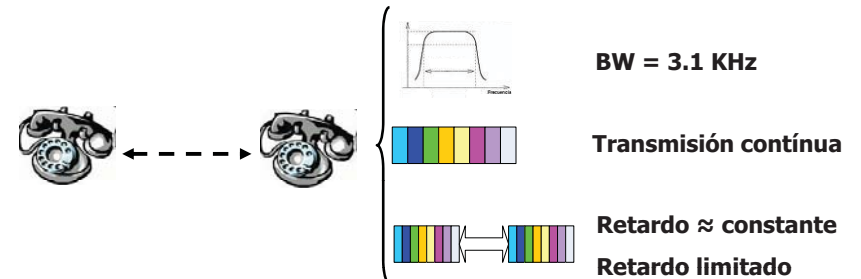
### ¿ Por qué ATM ?

- Antes de ATM (B-ISDN) cada aplicación requería de una red propia. La idea de una red unificada reduce costes de implementación y mantenimiento (ej. Es posible compartir el medio físico).
- Al mismo tiempo, al uso de la tecnología actual permite disponer de altas tasas de transferencia, siendo posible garantizar un nivel de prestaciones (QoS).

## 1. Introducción. Redes de banda ancha

### ▪ Introducción

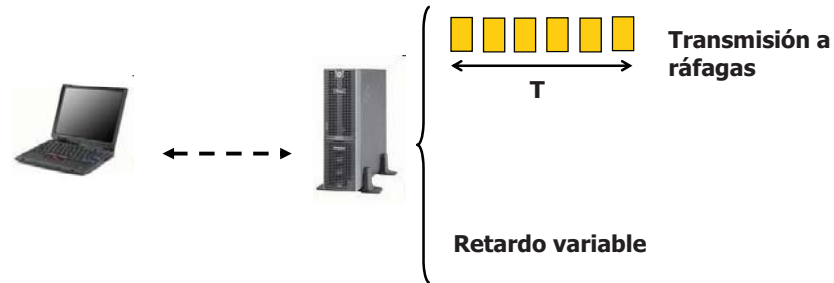
Sin embargo, unificar todos los servicios en una red no es sencillo, debido a la diferente naturaleza de la información y de las señales que se transmiten en cada caso.



# 1. Introducción. Redes de banda ancha

## ▪ Introducción

Sin embargo, unificar todos los servicios en una red no es sencillo, debido a la diferente naturaleza de la información y de las señales que se transmiten en cada caso.



# 1. Introducción. Redes de banda ancha

## ▪ Introducción

### Ventajas de ATM

- La RDSI de banda ancha o ATM, combina las redes de datos y las redes de telefonía en una única red. Esto proporciona las siguientes ventajas:
  - ✓ Se integran diferentes servicios (audio, video, datos, etc.) en una red que se adapta a las necesidades del tráfico (perfiles de tráfico).
  - ✓ Uso de componentes estándar. Lo que reduce los costes de despliegue, integración y mantenimiento.
  - ✓ Transmisión independiente del medio físico (de hecho, éste puede ser PDH, SDH, SONET..).

# 1. Introducción. Redes de banda ancha

## ▪ Introducción

### Ventajas de ATM

- ✓ Escalable. El ancho de banda puede adaptarse para cumplir los requisitos de aplicaciones futuras.
- ✓ Permite establecer una garantía de calidad de servicio (QoS).

# 1. Introducción. Redes de banda ancha

## ▪ Introducción

### Ventajas de ATM

- ✓ Escalable. El ancho de banda puede adaptarse para cumplir los requisitos de aplicaciones futuras.
- ✓ Permite establecer una garantía de calidad de servicio (QoS).



## 2. Modo de Transferencia Asíncrono (ATM)

### ¿ Qué es ATM ?

- ATM (*Asynchronous Transfer Mode*) es un método de comunicación de conmutación de circuitos que segmenta la información en paquetes de tamaño fijo denominados *celdas*. De hecho, la conmutación se realiza a este nivel.
- El uso de paquetes de tamaño fijo (*celdas*) es una de las principales de diferencias de ATM con otros sistemas de conmutación de paquetes como *X.25* o *Frame Relay*, donde se utilizan paquetes de tamaño variable.
- La utilización de paquetes de tamaño fijo permite realizar conmutar las celdas a gran velocidad.

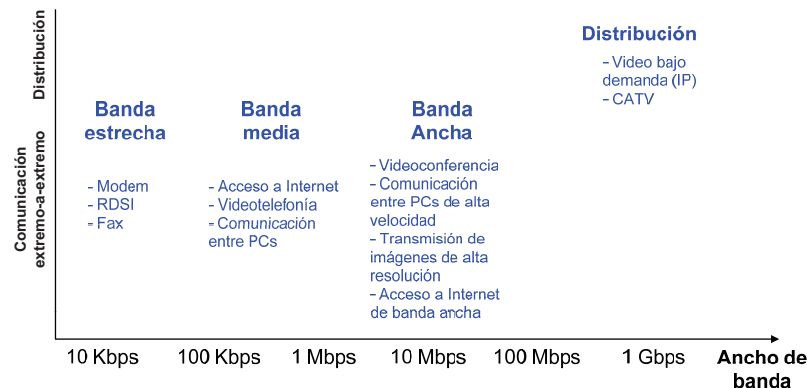
## 2. Modo de Transferencia Asíncrono (ATM)

### ¿ Por qué ATM ?

- A diferencia de las redes síncronas en las que existe una asignación de tiempo en la cual una aplicación o usuario puede transmitir (*ranura de tiempo* o *time-slot*), en ATM las celdas de un determinado equipo no ocupan una posición fija en una trama.
- En ATM, el ancho de banda utilizado por una determinada aplicación dependerá del número de celdas por unidad de tiempo que se transmitan.
- Estándar ATM. Dos organismos que trabajan conjuntamente:
  - ATM forum: asociación de fabricantes de equipos ATM
  - ITU-T: Organismo de estandarización

## 2. Modo de Transferencia Asíncrono (ATM)

### Nuevos servicios. Demanda de Ancho de banda



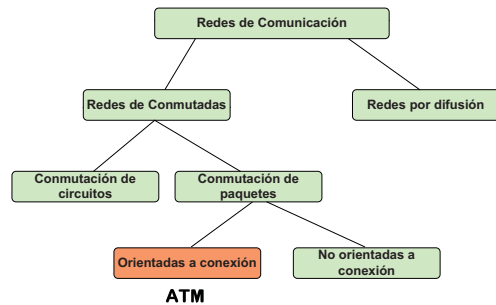
## 2. Modo de Transferencia Asíncrono (ATM)

### Evolución de las tecnologías de transporte

	1976	1988	1989
	X.25	Frame Relay	ATM
Multiplexación	STDM	STDM	STDM
Velocidad	Lineas alquiladas de 64 Kbps	Entre 56 Kbps y 1.544 Mbps	Hasta 10 Gbps
Control de errores	Salto a salto (paquete)	Extremo a extremo (paquete)	Extremo a extremo (sólo cabecera)
Manejo de la información	Por paquetes	Por ráfagas de paquetes	Por celdas
Tamaño paquetes	Variable	Variable	Fijo
Eficiencia	Velocidad y latencia dependientes del volumen de tráfico	Canal bidireccional con ancho de banda garantizado	Ancho de banda garantizado y baja latencia
Nivel OSI	3 (Red)	2 (Enlace)	2 (Enlace)
Ámbito	WAN servicios de baja velocidad (datos)	ISDN – WAN (datos)	WAN/LAN (datos, video voz)
Medio físico	Cobre	UTP / Fibra óptica	Fibra óptica

## 2. Modo de Transferencia Asíncrono (ATM)

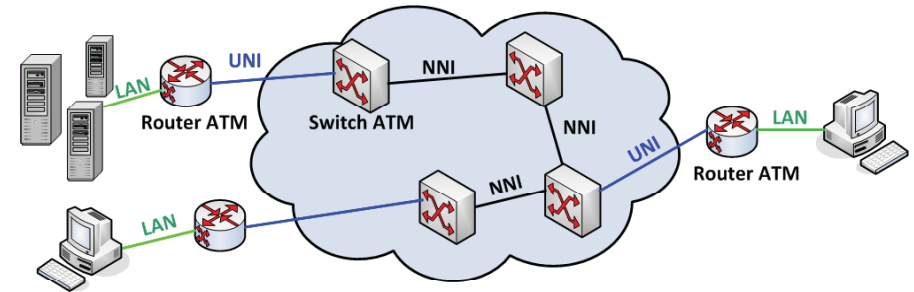
- Protocolo de retransmisión de paquetes (ATM Forum + ITU-T)



ATM es una red de conmutación de paquetes orientada a conexión, sobre la que se implementan circuitos lógicos. Esto permite combinar las ventajas de las redes de conmutación de circuitos (minimización del retardo y ancho de banda garantizado) junto con las ventajas de las redes de conmutación de paquetes (tasa de error limitada y uso eficiente del ancho de banda – multiplexación estadística)

## 2. Modo de Transferencia Asíncrono (ATM)

- En ATM se definen dos interfaces
  - Interfaz Usuario-Red (UNI)
  - Interfaz Red-Red (NNI)



- Los paquetes (celdas) en la red ATM difieren ligeramente en ambas interfaces

## 3. Transparencia en la transmisión

- Transparencia en la transmisión de la información

- Con la tecnología actual, es posible disponer de enlaces de datos de gran ancho de banda y de gran calidad, siendo posible reducir las funciones de detección y corrección de errores en los enlaces intermedios.
- De hecho, si es posible transferir información entre los límites de la red de forma transparente, es posible eliminar dichas funciones de detección y corrección de errores en cada nodo, recuciendo el tiempo de transmisión ( $\Rightarrow$  *transparencia temporal*).

## 3. Transparencia en la transmisión

- Transparencia semántica y temporal

- En la transferencia de información entre dos nodos debe garantizarse la transparencia:
  - Semántica: es decir, que la información se entregue al destino sin errores.
  - Temporal: es decir, que la información se entregue al destino sin retardos temporales.
- Cuando los enlaces de red son de mala calidad, es necesario implementar en los nodos funciones de detección y/o corrección de errores. Esto es lo que ocurre en las redes X.25, en las que en cada nodo se detectan y corrigen errores. El resultado es un tiempo de retardo muy alto en la transmisión, lo que hace que estas redes no fuesen útiles para transportar datos de servicios con restricciones temporales importantes (como voz u otros servicios de tiempo real).

### 3. Transparencia en la transmisión

#### ▪ Implementación de la transparencia

Cuando los enlaces de red son de mala calidad, es necesario implementar en los nodos funciones de detección y/o corrección de errores. Esto es lo que ocurre en las redes X.25, en las que en cada nodo se detectan y corrigen errores. El resultado es un tiempo de retardo muy alto en la transmisión, lo que hace que estas redes no fuesen útiles para transportar datos de servicios con restricciones temporales importantes (como voz u otros servicios de tiempo real).

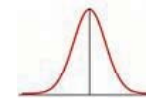
### 3. Transparencia en la transmisión

#### ▪ Transparencia temporal. Retardo

- En general, existen dos parámetros que contribuyen al retardo en una red.

1) Retardo de transferencia. Debido a la transmisión de la información desde la fuente al destino. Depende de la distancia entre la fuente y el destino ( $\sim 4$  ó  $5 \mu\text{s}/\text{Km}$ ).

2) Retardo por procesos. Debido a las operaciones realizadas en los diferentes nodos de la red (normalmente conmutación y multiplexación).

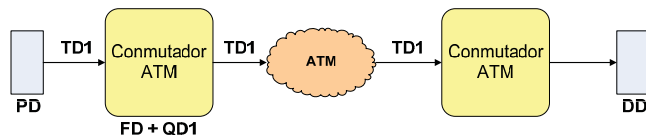


✓ *El retardo en la red se distribuye según una función de distribución gaussiana*

### 3. Transparencia en la transmisión

#### ▪ Transparencia temporal. Retardo

El retardo es un parámetro que afecta a la calidad de un servicio determinado. Por tanto, se define un límite superior para el retardo permitido en función del servicio.



Donde:

PD: Retardo por empaquetar    DD: Retardo por desempaquetar

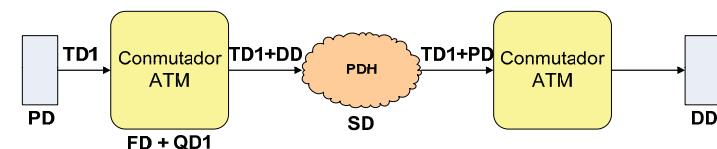
TD: Retardo de conmutación

QD: Retardo por uso de colas

### 3. Transparencia en la transmisión

#### ▪ Transparencia temporal. Retardo

- Si hubiese que atravesar otras redes no ATM para llegar al destino, habría además que añadir el retardo de dicha red así como el retardo asociado a empaquetar y desempaquetar a la entrada y a la salida de dicha red, respectivamente.



### 3. Transparencia en la transmisión

#### ▪ Transparencia temporal. Jitter

- El retardo ocasionado por los diferentes elementos de la red, hace que dicho retardo varíe para cada paquete. La variación *rápida* en el retardo para cada paquete recibe el nombre de *jitter*.
- Para eliminar el *jitter* se utilizan *buffers elásticos (de-jitter buffers)* intermedios donde se almacenan los paquetes, que son enviados a la siguiente etapa con una tasa constante (retardo constante entre los mismos)
- El máximo retardo que los *buffers* pueden compensar es igual al tiempo de retardo introducido por la fuente antes de comenzar a transmitir.

### 4. Celdas ATM

#### ▪ Paquetes transmitidos en la red ATM

- En ATM, la información se segmenta en paquetes de igual tamaño (53 bytes), denominados *celdas*, compuestos por una cabecera de 5 bytes y 48 bytes que representan la carga útil (para transportar información útil).
- El tamaño fijo de las *celdas* hace posible la conmutación de las mismas a gran velocidad.
- Por otro lado, en ATM se realiza una *multiplexación estadística*.

La rápida conmutación de las celdas junto con las ventajas de la *multiplexación estadística*, hace que ATM ofrezca las ventajas propias de las redes de *conmutación de circuitos* (transparencia temporal y ancho de banda garantizado) junto con las ventajas de las redes de *conmutación de paquetes* (transparencia semántica y uso eficiente del ancho de banda).

### 4. Celdas ATM

#### ▪ Características principales de la red ATM

- Red asíncrona
- Multiplexación estadística ⇒ Eficiencia en el ancho de banda
- Multiplexación de paquetes (celdas) de tamaño fijo (53 bytes)
- Orientado a conexión
- La funcionalidad de la cabecera es reducida
- No hay recuperación de errores ni control de flujo entre los enlaces (los enlaces se suponen de gran calidad).

### Multiplexación estadística

- Permite aprovechar los recursos físicos disponibles
- Método de multiplexación típico en redes de conmutación de paquetes (TDM asíncrono)

En las redes síncronas (ej. conmutación de circuitos) donde se utilizan técnicas de multiplexación temporal (TDM), se asegura un ancho de banda fijo e igual para cada conexión. Para ello, se asigna una (o varias) ranura temporal de uso exclusivo para un usuario.

**Se desperdicia el ancho de banda asignado a un usuario si no tiene nada que transmitir**



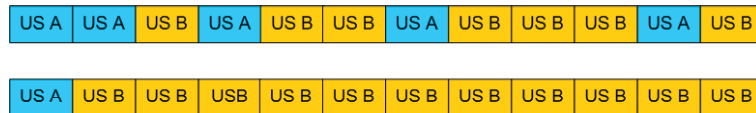
## 4. Celdas ATM

### ▪ Multiplexación estadística

- Permite aprovechar los recursos físicos disponibles
- Método de multiplexación típico en redes de conmutación de paquetes

La multiplexación estadística o TDM asíncrona minimiza el número de ranuras vacías en la red, basándose en la velocidad de transferencia variable de los flujos individuales → Reparte el total de ranuras disponibles entre los usuarios que tienen datos para ser transmitidos.

**Como desventaja, no garantiza un reparto equitativo de recursos entre los usuarios**



## 4. Celdas ATM

- Los paquetes que se transmiten en la red ATM se denominan *celdas*
- Son unidades de tamaño pequeño y fijo con una cabecera de funcionalidad reducida

¿ Qué ventaja tiene el uso de paquetes de tamaño pequeño y fijo ?

¿ Qué ventaja tiene la cabecera de funcionalidad reducida?

## 4. Celdas ATM

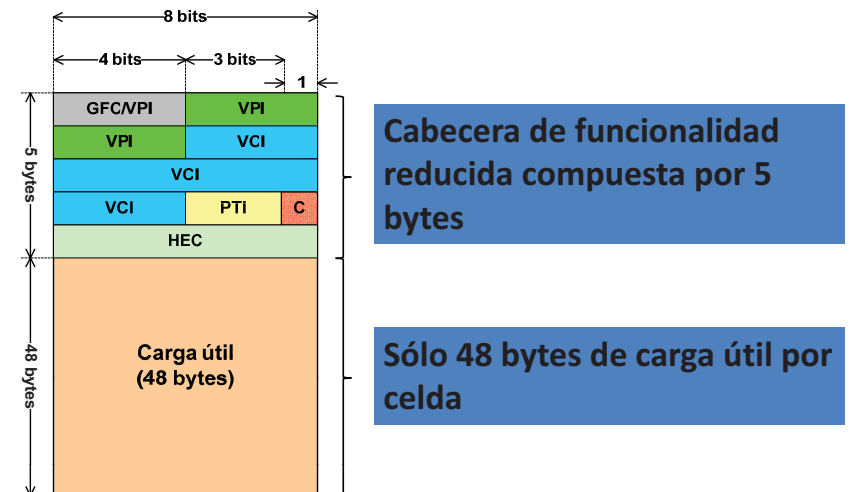
- Los paquetes que se transmiten en la red ATM se denominan *celdas*
- Son unidades de tamaño pequeño y fijo con una cabecera de funcionalidad reducida

¿ Qué ventaja tiene el uso de paquetes de tamaño pequeño y fijo ?  
¿ Qué ventaja tiene la cabecera de funcionalidad reducida?

Se consigue que el tráfico sea muy predecible y pueda realizarse la conmutación de manera muy eficiente (hardware)  
*La rápida conmutación de las celdas junto con las ventajas de la multiplexación estadística hace que ATM ofrezca ventajas de las redes de conmutación de circuitos y de las redes de conmutación de paquetes*

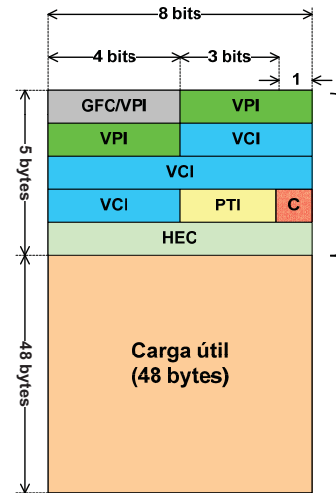
## 4. Celdas ATM

### ▪ Formato de las celdas ATM



## 4. Celdas ATM

### Formato de las celdas ATM. Cabecera

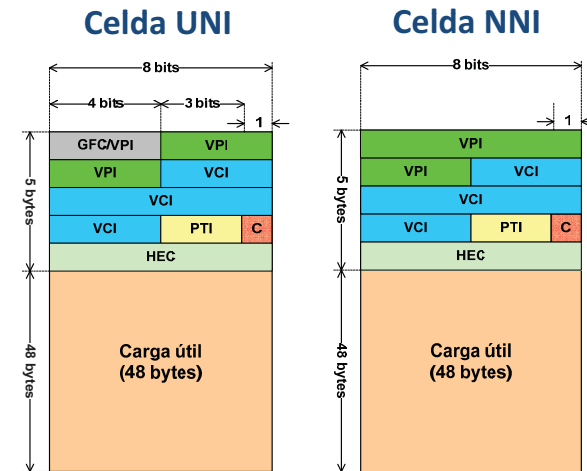


▪ **GFC (Generic Flow Control)**. Se utiliza en la interfaz UNI para gestionar la multiplexación y el control de flujo entre celdas pertenecientes a diferentes conexiones.

En la práctica, estos 4 bits están a 0 al no estar estandarizados los valores de este campo y se utiliza en la interfaz red-red (NNI), para ampliar el campo VPI.

## 4. Celdas ATM

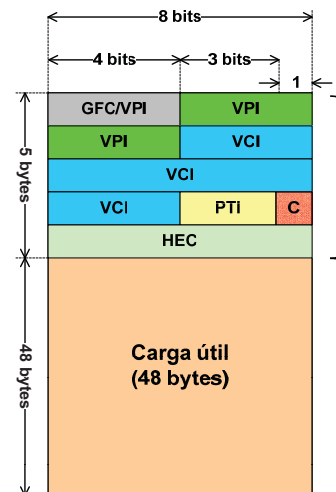
### Formato de las celdas ATM. Cabecera



En la interfaz NNI se utilizan 8 bits para el campo VPI, ampliando el número de nodos direccionables.

## 4. Celdas ATM

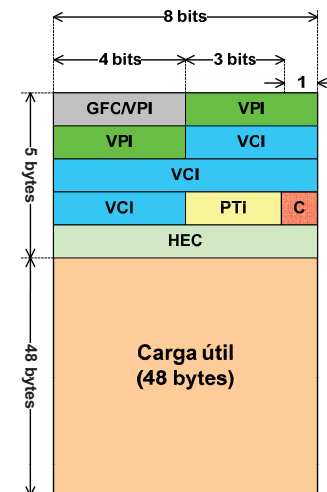
### Formato de las celdas ATM. Cabecera



▪ **VPI (Virtual Path Identifier)**. Contiene la segunda parte de la dirección (camino virtual). El VPI comprende varios canales virtuales (VCI) y permite la rápida conmutación de las células en la red (conmutadores ATM).

## 4. Celdas ATM

### Formato de las celdas ATM. Cabecera



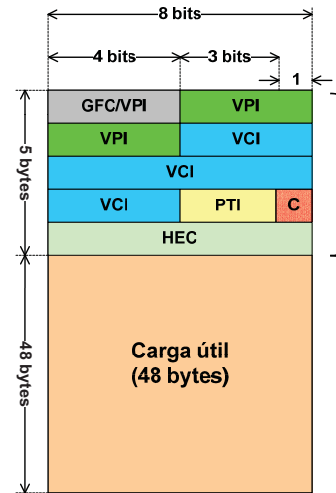
▪ **VCI (Virtual Channel Identifier)**. El campo VCI contiene parte de la información de dirección. Todas las células que pertenecen al mismo canal virtual circularán por el mismo VCI. El campo VCI identifica la parte del camino entre dos conmutadores ATM o entre un conmutador y el abonado. El conjunto de canales virtuales por los cuales circula una célula entre dos extremos de la red, marcan el camino virtual.

Los campos **VPI** y **VCI** los asigna el conmutador ATM durante el establecimiento de la llamada (*call-setup*).



## 4. Celdas ATM

### Formato de las celdas ATM. Cabecera

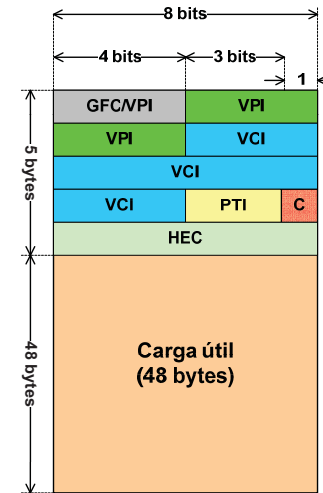


▪ **PTI (Payload Type Indicator)**. Indica el tipo de datos que contiene la carga útil (*payload*) de la célula. Este campo se utiliza para diferenciar entre información de control o de usuario, para mantenimiento, administración y control de congestión.

Los valores que pueden tomar los 3 bits del campo PTI están indicados en el estándar (ITU-T, I.150)

## 4. Celdas ATM

### Formato de las celdas ATM. Cabecera



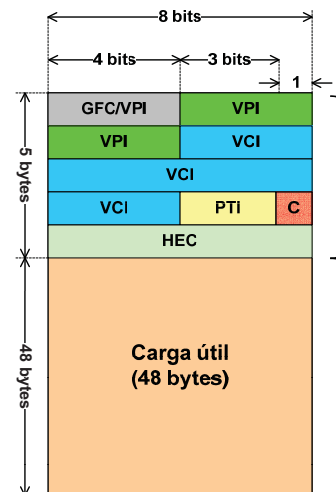
▪ **PTI (Payload Type Indicator)**.

PTI	Uso	Descripción
000	US	Sin congestión, SDU tipo 0
001	US	Sin Congestión, SDU tipo 1
010	US	Congestión, SDU tipo 0
011	US	Congestión, SDU tipo 1
100	AD	Celda OAM F5 – Flujo segmento
101	AD	Celda OAM F5 – Flujo extremo-extremo
110	RS	Reservado para uso futuro
111	RS	Reservado para uso futuro

SDU tipo 1 → Celda final de segmento CS

## 4. Celdas ATM

### Formato de las celdas ATM. Cabecera

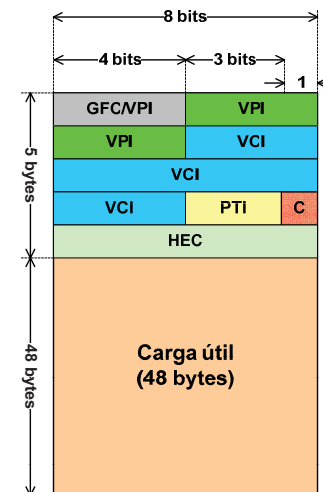


▪ **CLP (Cell Loss Priority)**. Mediante el bit CLP se indica a la red si la célula es prioritaria o no, en cuyo caso, puede ser eliminada de la red en el caso de problemas de congestión. Las células con CLP=0 tienen una mayor prioridad que las células con CLP=1.

El campo CLP juega un papel importante en la gestión del tráfico de los diferentes servicios transportados por la red ATM

## 4. Celdas ATM

### Formato de las celdas ATM. Cabecera



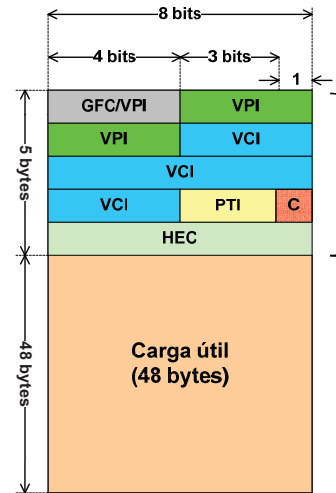
▪ **HEC (Header Error Control)**. Este campo se utiliza para controlar, y en algunos casos corregir, errores en la cabecera. Además, el campo HEC se utiliza para sincronizar el receptor, haciendo posible la detección del inicio de una celda. Es un CRC de 8 bits calculado sobre los 4 primeros bytes de la cabecera.

➤ Se utiliza el polinomio generador  $x^8+x^2+x+1$

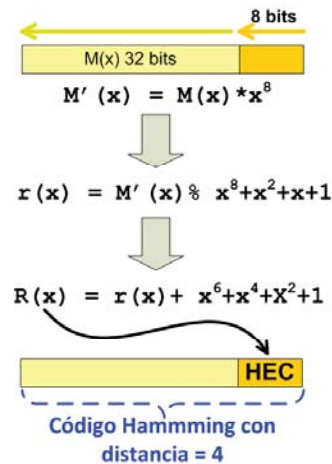
El campo HEC se utiliza además en el proceso de alineamiento de celdas

## 4. Celdas ATM

### Formato de las celdas ATM. Cabecera



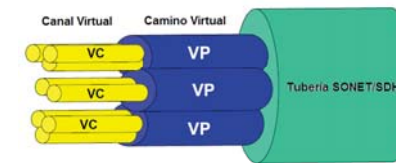
### Proceso de cálculo del HEC



## 5. Conexiones virtuales

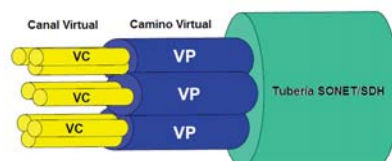
### Caminos y canales virtuales en ATM

- En ATM, las celdas se transfieren utilizando rutas extremo a extremo conocidas como conexiones virtuales, que se identifican mediante los campos VCI y VPI de la cabecera (de hecho, esta es la función principal de la cabecera).
- Cada enlace físico soporta miles de conexiones virtuales, dependiendo de las necesidades de tráfico.
- La conexión entre diferentes conexiones virtuales son los caminos y canales virtuales.



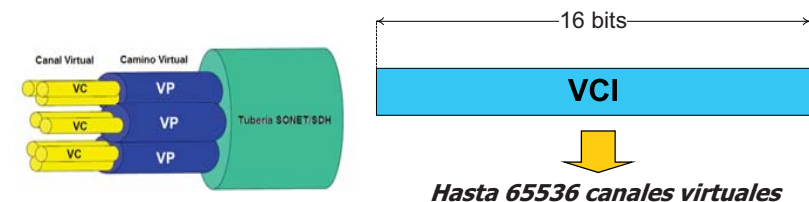
## 5. Conexiones virtuales

- El tráfico generado por diferentes fuentes se agrupa en una tubería que llegará hasta el destino.
- Una *tubería ATM* es un *camino virtual (VP)*, un conjunto de circuitos en un enlace de red.
- Diferentes canales pueden pedir conexiones con destinos específicos. Dichos canales (VC) no son fijos en todo el trayecto entre fuente y destino (pueden pasar de un VP a otro).



## 5. Conexiones virtuales

- Los enlaces de fibra óptica pueden transportar un gran número de canales. Por esta razón, es necesario un identificador de canal virtual con la longitud necesaria.
- El identificador de canal virtual VCI se asigna al inicio de la conexión (*call-setup*) y sólo tiene significado local para un enlace entre nodos ATM (*conmutación de VCI*).
- Pueden utilizarse más de VCI para servicios con diferentes fuentes de tráfico.



## 6. Control de errores en ATM

- En redes donde se utilizan **enlaces de red de baja calidad**, es necesario implementar **procedimientos de detección y corrección de errores nodo a nodo**

¿ Qué ocurriría si dispusiéramos de enlaces de gran calidad (baja probabilidad de error) ?

## 6. Control de errores en ATM

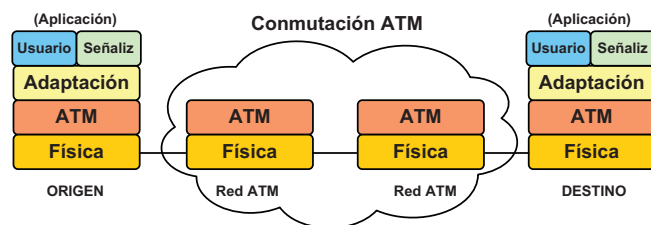
- En redes donde se utilizan **enlaces de red de baja calidad**, es necesario implementar **procedimientos de detección y corrección de errores nodo a nodo**

¿ Qué ocurriría si dispusiéramos de enlaces de gran calidad (baja probabilidad de error) ?

Se podrían eliminar las funciones de detección/corrección de error nodo a nodo e implementarlas sólo en los extremos

## 6. Control de errores en ATM

- Los **nodos ATM** sólo implementan hasta el **nivel 2**

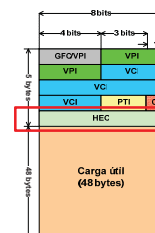


- Las funciones de **detección/corrección de errores** así como el control de flujo se implementa en capas superiores (sólo en los extremos)

ATM es una red de retransmisión de celdas (cell-relay)

## 6. Control de errores en ATM

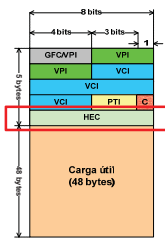
- En **ATM no se realiza ningún tipo de control de integridad de los datos de usuario** que transportan las celdas



Entonces, ¿ por qué hay un campo de control de errores en la cabecera (HEC) ?

## 6. Control de errores en ATM

- En ATM no se realiza ningún tipo de control de integridad de los **datos de usuario** que transportan las celdas

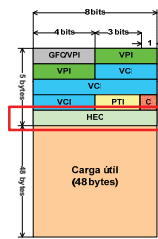


Entonces, ¿por qué hay un campo de control de errores en la cabecera (HEC) ?

El campo HEC protege sólo la cabecera

## 6. Control de errores en ATM

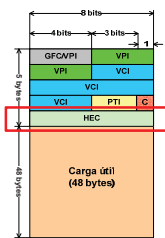
- En ATM no se realiza ningún tipo de control de integridad de los **datos de usuario** que transportan las celdas



Y, ¿Por qué se protege sólo la cabecera ?

## 6. Control de errores en ATM

- En ATM no se realiza ningún tipo de control de integridad de los **datos de usuario** que transportan las celdas



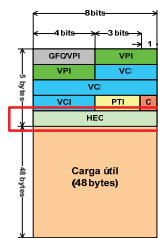
Y, ¿Por qué se protege sólo la cabecera ?

¿ Qué contiene la cabecera para que sea tan importante protegerla ?

Información de direccionamiento de las celdas

## 6. Control de errores en ATM

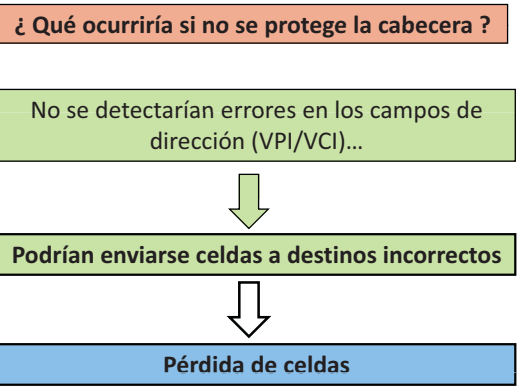
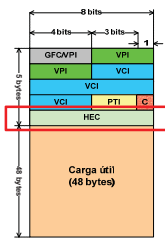
- En ATM no se realiza ningún tipo de control de integridad de los **datos de usuario** que transportan las celdas



¿ Qué ocurriría si no se protege la cabecera ?

## 6. Control de errores en ATM

- En ATM no se realiza ningún tipo de control de integridad de los datos de usuario que transportan las celdas



## 6. Control de errores en ATM

- Pérdida de celdas por errores en VPI/VCI

- El campo HEC de la cabecera es un CRC de 8 bits calculado sobre los 32 primeros bits de la cabecera
- Su principal misión es proteger los campos VPI/VCI para evitar el direccionamiento a un destino incorrecto

Un CRC de 8 bits permite detectar errores simples o múltiples y corregir errores simples

- Error múltiple → celda descartada por ser errónea. No produce efecto en la red
- Error simple → Si éste está en la cabecera, puede alterar los campos VPI/VCI, encaminando a un destino incorrecto

## 6. Control de errores en ATM

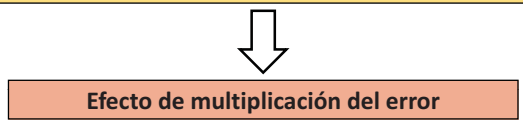
- Pérdida de celdas por errores en VPI/VCI

- Efecto de multiplicación del error

Cuando hay un error simple en los campos VPI/VCI puede ocurrir:

a) La dirección errónea no exista en la red. La celda se pierde, afectando sólo a una conexión (destino)

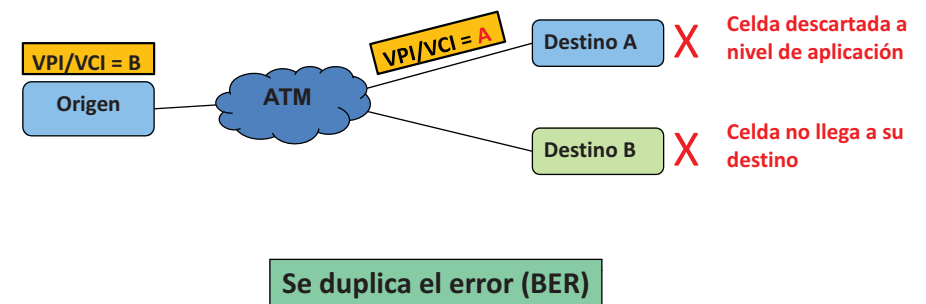
b) La dirección errónea existe. La celda se encamina a un destino incorrecto



## 6. Control de errores en ATM

- Efecto de multiplicación del error (me)

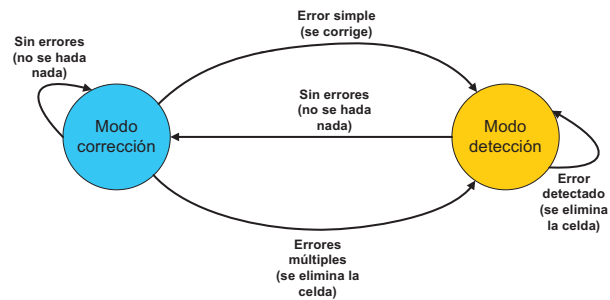
- Efecto de enviar una celda a un destino incorrecto



## 6. Control de errores en ATM

### ▪ Protección frente a me

- Se utiliza un algoritmo adaptativo
  - Está basado en la comprobación del campo HEC

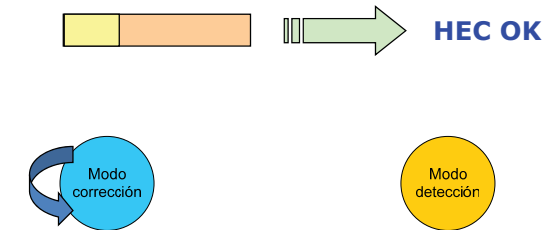


Se asume que los errores aparecen en ráfagas  
Los mecanismos de control de flujo (retransmisión)  
se implementan a nivel de aplicación

## 6. Control de errores en ATM

### ▪ Protección frente a me

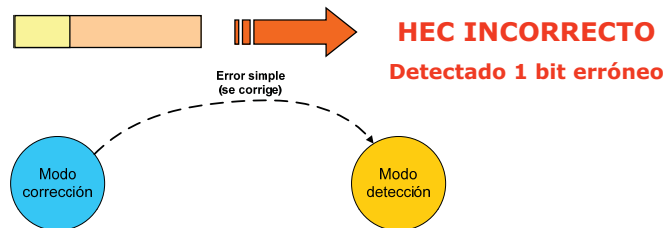
- Por defecto, el receptor estará en modo corrección y permanecerá en él hasta que se detecte un error.



## 6. Control de errores en ATM

### ▪ Protección frente a me

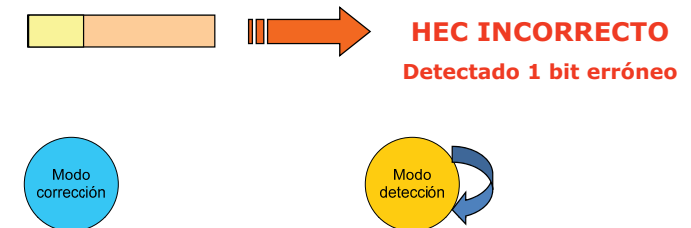
- Si se detecta un error simple, el receptor lo corrige y pasa al modo detección.



## 6. Control de errores en ATM

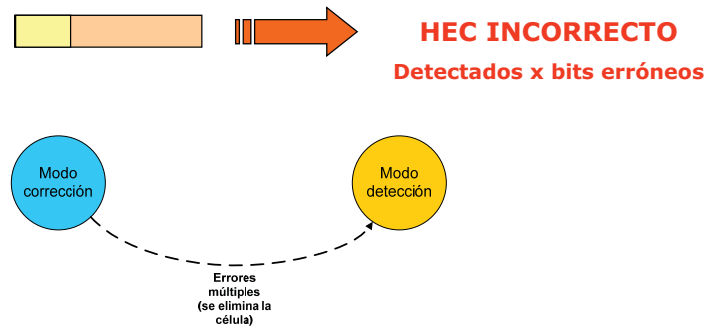
### ▪ Protección frente a me

- El receptor permanece en modo detección y descarta todas las celdas consecutivas erróneas (incluso con error simple)



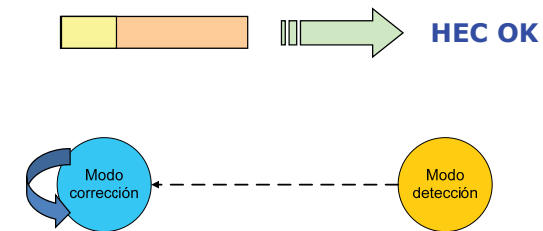
## 6. Control de errores en ATM

- Protección frente a me
- Si se detecta un error múltiple, el receptor descarta la celda y pasa a modo detección.



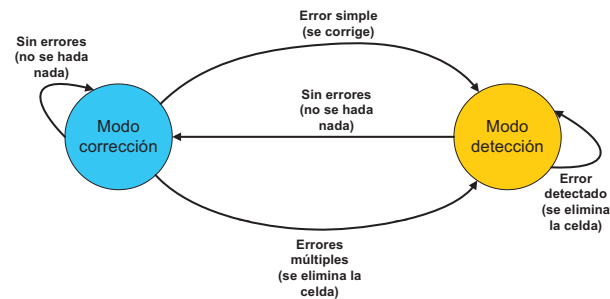
## 6. Control de errores en ATM

- Protección frente a me
- Cuando se recibe la primera celda correcta, el receptor vuelve a modo corrección.



## 6. Control de errores en ATM

- Protección frente a me
- Se utiliza un algoritmo adaptativo
  - Está basado en la comprobación del campo HEC



## 7. Delineación de celdas

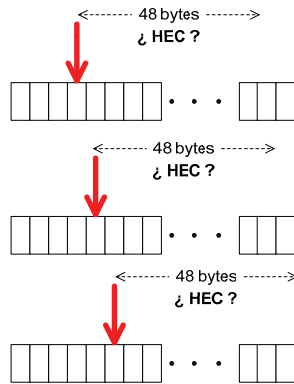
- Es el proceso de sincronización en ATM

Si ATM es asíncrono, ¿ en qué consiste el proceso de sincronización?

Los nodos ATM no están siempre sincronizados entre sí (sistema asíncrono), como ocurre en las redes síncronas. Se sincronizan para poder enviar o recibir datos – conectarse a la red - (no es necesario que todos los nodos compartan una señal de reloj)

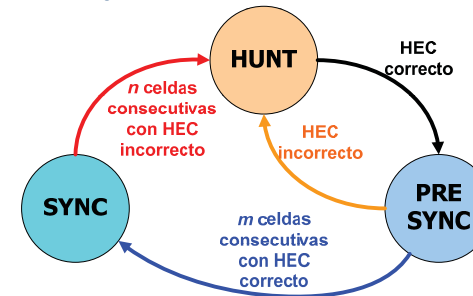
## 7. Delineación de celdas

- Inicialmente, se comprueba el HEC bit a bit buscando el inicio de una celda



## 7. Delineación de celdas

- Para dar estabilidad al sincronismo, se utiliza una máquina de estados



Según el estándar (I.432.1),  
 $n=7, m=6$

El algoritmo de delineación de celdas evita falsas sincronizaciones debidas a combinaciones aleatorias en el flujo de bits. Una vez sincronizado el receptor, tienen que detectarse  $n$  celdas consecutivas con HEC correcto para que el sincronismo se pierda. Esta máquina de estados proporciona estabilidad al sincronismo.

## 7. Delineación de celdas

¿Cuál es la probabilidad de que la comprobación de HEC resulte correcta por una combinación aleatoria de bits ?

## 7. Delineación de celdas

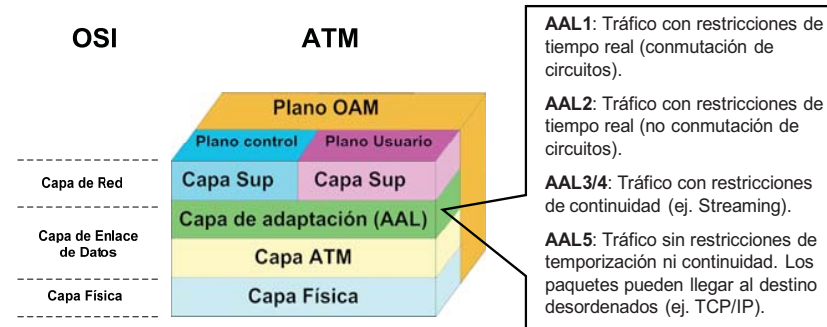
¿Cuál es la probabilidad de que la comprobación de HEC resulte correcta por una combinación aleatoria de bits ?

La cabecera contiene un CRC-8, por tanto, la probabilidad de que no se detecte un error es de  $1/2^8=0.004$



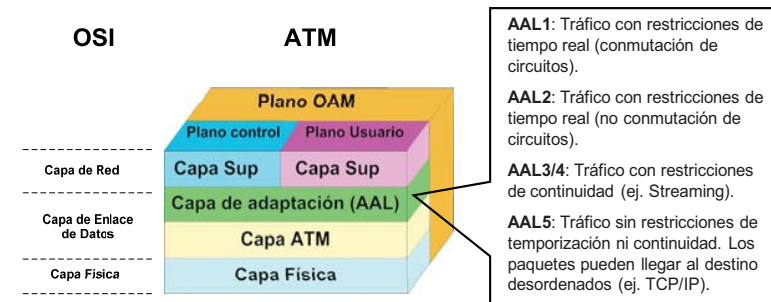
## 8. Modelo de Referencia ATM

- ATM es un protocolo de nivel 2 basado en la retransmisión de celdas
- Para poder transmitir datos de diferentes servicios, es necesaria una capa de adaptación (AAL)

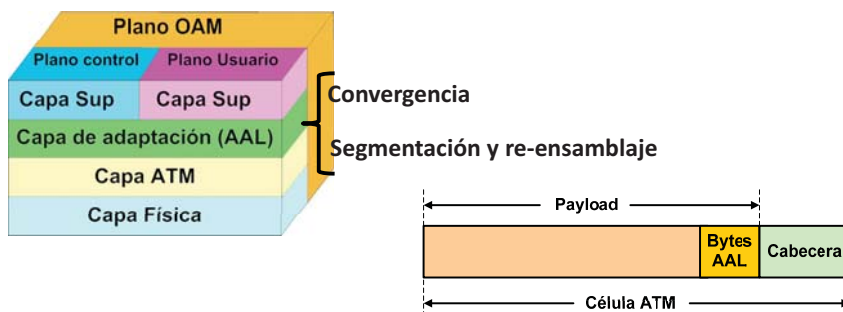


## 8. Modelo de Referencia ATM

- En el modelo de referencia, diferenciamos 3 planos:
  - Usuario → responsable de la transferencia de datos de usuario
  - Control → responsable de los mensajes de señalización
  - OAM → Detección de fallos de red, fallos de protocolo y gestión de nodos

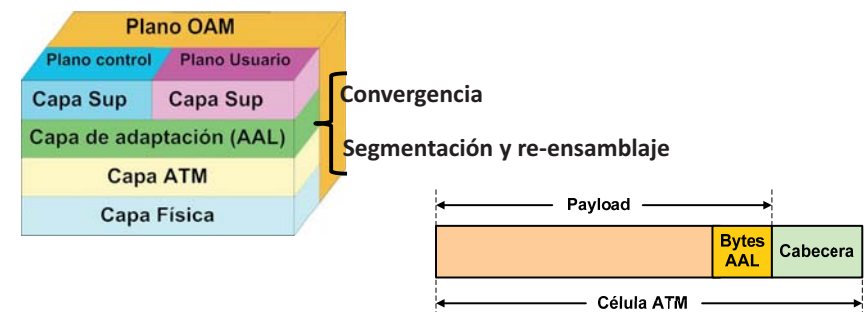


## 8. Modelo de Referencia ATM



**Subnivel CS (Convergence Sublayer).** Envuelve la SDU (Service Data Unit) de usuario con una cabecera con la información necesaria para suministrar los servicios requeridos. Esta información depende de la clase de servicio transportada. Normalmente, contiene información para garantizar el control de errores y la sincronización de la información.

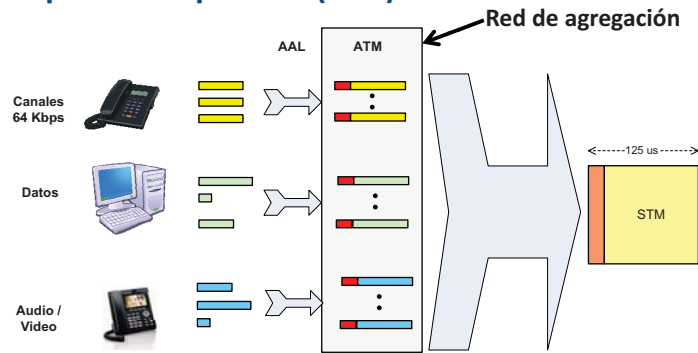
## 8. Modelo de Referencia ATM



**Subnivel SAR (Segmentation and Reassembly).** Este nivel recibe la SDU del subnivel de convergencia y la divide en segmentos que pueden ser alojados dentro de una célula. A estos segmentos se les añade una cabecera con la información necesaria para el re-ensamblaje en el destino.

## 8. Modelo de Referencia ATM

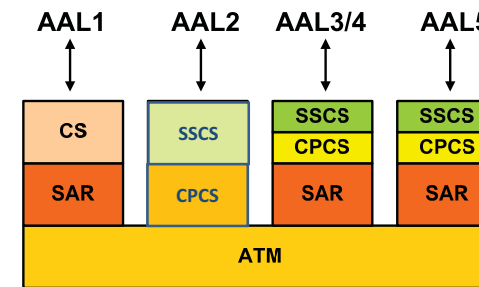
### Capa de Adaptación (AAL)



La capa AAL es la interfaz entre la capa ATM y las capas superiores. Dividirá los paquetes de las capas superiores en celdas, podrá detectar errores y transportará información temporal para que el destino pueda generar señales dependientes del tiempo (ej. servicios de tiempo real).

## 8. Modelo de Referencia ATM

### Capa de Adaptación (AAL)



**AAL1:** Tráfico con restricciones de tiempo real (conmutación de circuitos).

**AAL2:** Tráfico con restricciones de tiempo real (no conmutación de circuitos).

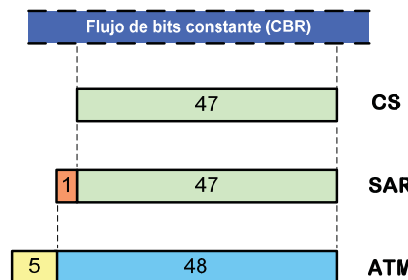
**AAL3/4:** Tráfico con restricciones de continuidad (ej. Streaming). (en desuso)

**AAL5:** Tráfico sin restricciones de temporización ni continuidad. Los paquetes pueden llegar al destino desordenados (ej. TCP/IP).

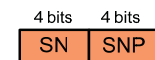
SSCS → Service Specific CS  
CPCS → Common Part CS

## 8. Modelo de Referencia ATM

### Capa AAL 1



#### Cabecera SAR

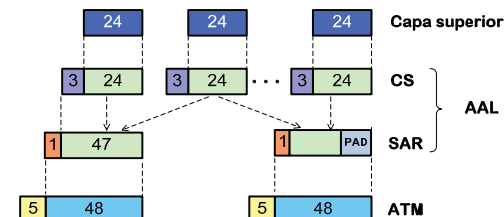


SN: Número de secuencia  
SNP: Protección del número de secuencia (CRC)

- Introduce 1 bit de redundancia en la capa SAR
- Supone que hay un flujo constante de información (tráfico CBR)
- Transporte de señales RDSI, audio/video CBR y emulación de circuitos

## 8. Modelo de Referencia ATM

### Capa AAL 2

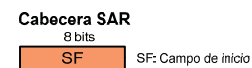


- Introduce 4 bytes de información de control por celda
- Servicios orientados a conexión, de tasa binaria variable y con restricciones temporales

- Ej. Vídeo comprimido, Transporte de GSM EDGE Radio Access Network - Núcleo de red (UTRAN/GERAN-CN) y red troncal de telefonía móvil (RTMC)

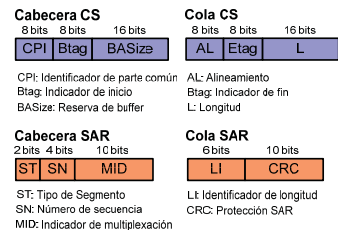
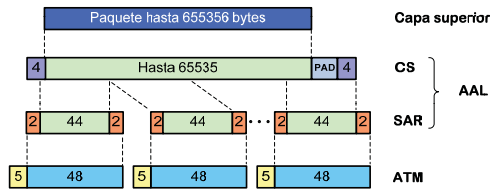


CID: Identificador de canal UUI: Indicador usuario-a-usuario  
LI: Indicador de longitud CRC: Control de error de cabecera CS  
PPT: Tipo de payload



## 8. Modelo de Referencia ATM

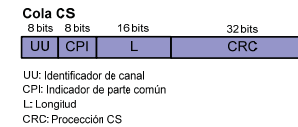
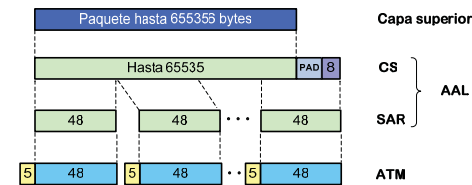
### ▪ Capa AAL 3/4



- Introduce 4 bytes de información de control por celda
- Servicios orientados y no orientados a conexión, sin restricciones temporales
- Ej. Tráfico asíncrono, X.25

## 8. Modelo de Referencia ATM

### ▪ Capa AAL 5



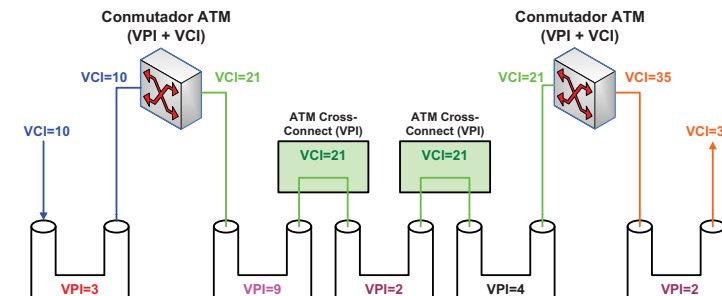
- Introduce 8 bytes de información de control por trama que se transmiten en la última celda
- Es la capa menos restrictiva
- El bit PTI indica que se trata de la última celda
- Diseñado para el transporte de TCP/IP – IP sobre ATM

## 9. Conmutación en ATM

- ATM ofrece las ventajas propias de las redes de conmutación de circuitos y de las redes de conmutación de paquetes. Por tanto, ATM es una tecnología de *conmutación de circuitos*. Esto quiere decir, que debe establecerse un camino en la red antes de que pueda transferirse información entre dos extremos, igual que ocurre en una red telefónica conmutada.
- La diferencia esencial con una red telefónica conmutada es que en ATM los circuitos conmutados son *virtuales*, es decir, no son circuitos físicos. Dichos circuitos aparecen en las tablas de rutas de los conmutadores ATM.

## 9. Conmutación en ATM

Un VPI indica un camino virtual, que puede recoger varios canales virtuales (varios VCI).



## 10. Gestión del tráfico

### ▪ Gestión del tráfico

- Gestión de tráfico o control de congestión.
- ATM no realiza ni corrección de errores ni control de flujo.
- Para un buen funcionamiento, el usuario y la red se tienen que poner de acuerdo en cómo van a transmitir.
- El usuario:
  - describe las características de su tráfico
  - pide unas **una calidad de servicio** a la red
- La red:
  - **Admite el tráfico** de usuario si, dadas las características de éste, puede cumplir la calidad pedida.
  - **Monitoriza** que el tráfico cumple con las características especificadas.

## 10. Gestión del tráfico

### ▪ Descriptores de tráfico

Un descriptor de tráfico consiste en un conjunto de parámetros que definen las características que debe cumplir una conexión para una determinada categoría de servicio.

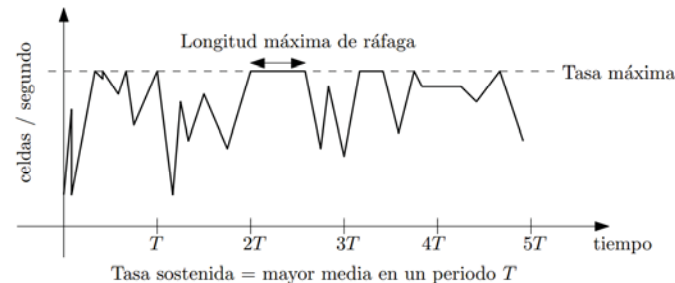
Los descriptores de tráfico son necesarios para asegurar la asignación de recursos y garantizar la calidad de servicio a través de la red ATM.

## 10. Gestión del tráfico

### ▪ Descriptores de tráfico

Una fuente ATM debe especificar el tráfico que genera mediante los siguientes descriptores:

- 1) **Peak Cell Rate (PCR)**. Representa la tasa de transferencia pico de la fuente, es decir, la velocidad instantánea máxima a la que el usuario puede transmitir. El tiempo mínimo entre llegadas de las celdas puede calcularse como  $1/PCR$ . Análogamente se define el **minimum cell rate**.



## 10. Gestión del tráfico

### ▪ Descriptores de tráfico

- 2) **Sustained Cell Rate (SCR)**. Representa la tasa medida en un intervalo grande de tiempo. Se utiliza en algunas conexiones para incrementar la eficiencia de la red y la ganancia estadística.
- 3) **Minimum Cell Rate (MCR)**. Es la tasa de transmisión mínima deseada por un usuario.
- 4) **Maximum Burst Size (MBS)**. Es el número máximo de celdas consecutivas que se pueden enviar a la tasa de pico sin violar la tasa media (SCR). Este parámetro se puede calcular:

$$Burst\ Tolerance = (MBS - 1) \left( \frac{1}{SCR} - \frac{1}{PCR} \right)$$

## 10. Gestión del tráfico

### ▪ Burtstiness para diferentes servicios

Servicio	$E[s(t)]$	B
Voz	32 Kbit/s	2
Datos interactivos	1-100 kbit/s	10
Datos (bulk)	1-10 Mbit/s	1-10
Video – calidad estándar	1.5 – 15 Mbit/s	2-3
Video – HD (HDTV)	15 – 150 Mbit/s	1-2
Videotelefonía alta calidad	0.2 – 2 Mbit/s	5

## 10. Gestión del tráfico

### ▪ Perfiles de tráfico

- Un perfil de tráfico es una clase de calidad de servicio, y está asociada a un conjunto de parámetros de tráfico y un conjunto de parámetros de calidad de servicio. El perfil se comunica durante el establecimiento de la conexión, al igual que los descriptores de tráfico y calidad de servicio.
- Existen los siguientes perfiles:
  - CBR: Constant bit rate
  - rt-VBR: Real time variable bit rate
  - nrt-VBR: non-real time variable bit rate
  - ABR: available bit rate
  - UBR: unspecified bit rate

*No se especifica correspondencia entre perfiles de tráfico y capas de adaptación.*

## 10. Gestión del tráfico

### ▪ Categoría de servicios en función del perfil de tráfico

ATM-FORUM	ITU-T	Perfil de Tráfico	Aplicación
CBR	DBR		Tasa de bit constante con referencias temporales <i>Voz, video</i>
rt-VBR	-		Tasa de bit variable con referencias temporales <i>Voz, video comprimidos</i>

## 10. Gestión del tráfico

### ▪ Categoría de servicios en función del perfil de tráfico

ATM-FORUM	ITU-T	Perfil de Tráfico	Aplicación
Nrt-VBR	SBR		Tasa de bit constante sin referencias temporales <i>Transferencia de ficheros</i>
ABR	ABR		Asignación de ancho de banda adaptativo, dependiendo de los recursos

## 10. Gestión del tráfico

### ▪ Categoría de servicios en función del perfil de tráfico

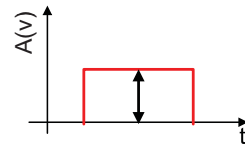
ATM-FORUM

ITU-T

Perfil de Tráfico

Aplicación

UBR



Sin garantía de tasa de bit ni QoS

## 10. Gestión del tráfico

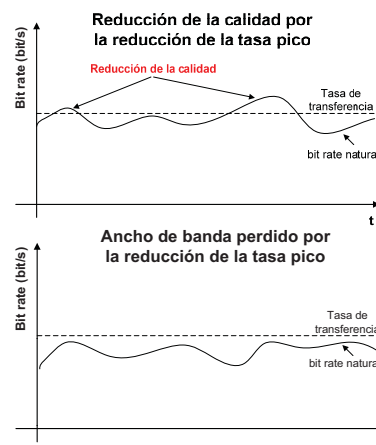
### ▪ Categoría de servicios y aplicaciones

	CBR	Rt-VBR	Nrt-VBR	ABR	UBR
Datos críticos	●●	●	●●●	●	○
LAN	●	●	●●	●●●	●●
Transporte WAN	●	●	●●	●●●	●●
Emulación de circuitos	●●●	●●	○	○	○
Telefonía, Videotelefonía	●●●	○○	○○	○	○
Audio comprimido	●	●●●	●●	●●	●
Distribución de vídeo	●●●	●●●	●	○	○
Servicios multimedia interactivos	●●●	●●●	●●	●●	●

●●● Óptimo ; ●● Bueno ; ● Moderado ; ○ No apropiado ; ○○ Bajo revisión

## 10. Gestión del tráfico

### ▪ Ancho de banda dinámico



## 10. Gestión del tráfico

### ▪ Calidad de servicio

- Los servicios proporcionados por ATM pueden clasificarse de acuerdo a diferentes criterios:
  - 1) Tipo de servicio, caracterizado por los parámetros del tráfico
  - 2) Calidad del servicio, caracterizado por los parámetros QoS
- Las características del tráfico deben ser aceptadas antes de que la comunicación comience (*contrato de tráfico*).

## 10. Gestión del tráfico

### ▪ Parámetros de calidad de servicio

#### 1) Cell Loss Ratio (CLR)

Es el porcentaje de celdas perdidas en la red debido a problemas de congestión.

$$CLR = \frac{\text{Células Perdidas}}{\text{Células Transmitidas}}$$

Es el porcentaje de celdas perdidas en la red debido a problemas de congestión. Cada celda ATM contiene el bit CLP en la cabecera. En situaciones de congestión, las celdas con el bit CLP=1 se descartan. CLR puede definirse por separado para celdas con CLP=1 y para celdas con CLP=0.

## 10. Gestión del tráfico

### ▪ Parámetros de calidad de servicio

#### 2) Cell Transfer Delay (CTD)

Es el retraso experimentado por una celda en la red. Este retraso se debe al tiempo de propagación en la red, a las colas en los conmutadores y a los tiempos de servicio.

#### 3) Cell Delay Variation (CDV)

Es una medida de la varianza del CTD. Una alta varianza en el CTD implica tener colas de gran tamaño, las cuales provocan problemas en tráfico de voz y vídeo. Existen múltiples formas de medir el CDV. Una de ellas consiste en medir el denominado CDV pico-a-pico, calculando la diferencia entre el  $(1-\alpha)$ -percentil y el valor mínimo de CTD para un valor pequeño de  $\alpha$ .

## 10. Gestión del tráfico

### ▪ Control de admisión de conexiones (CAC)

El CAC es una función del conmutador que determina si una conexión debe ser aceptada o rechazada, asegurando la calidad de servicio de las demás conexiones así como la calidad de servicio demandada por la nueva conexión.

El control de admisión utiliza los siguientes parámetros:

- 1) Descriptor de tráfico
- 2) Calidad de servicio de la conexión solicitada
- 3) Calidad de servicio de las conexiones ya aceptadas
- 4) Anchos de banda ya asignados
- 5) Ocupación de las colas

## 10. Gestión del tráfico

### ▪ Monitorización del tráfico

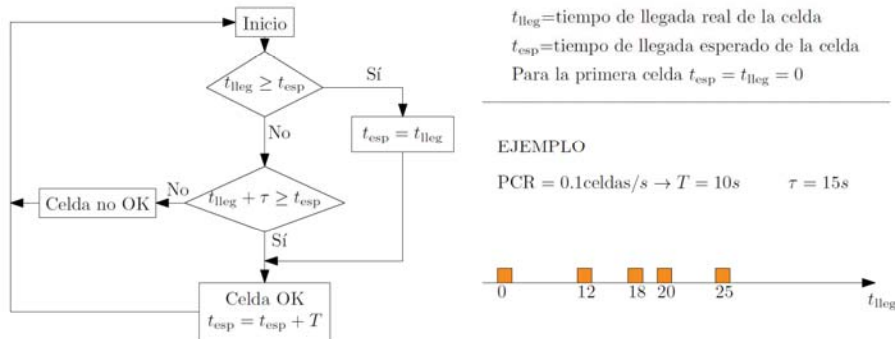
▪ El tráfico debe comportarse de acuerdo a la definición realizada durante la petición de conexión mediante el descriptor de tráfico. La vigilancia del cumplimiento de dicho compromiso recae sobre los algoritmos GCRA (Generic Cell Rate Algorithms), que se aplican a los parámetros que forman el descriptor de tráfico.

▪ Mediante los algoritmos GCRA es posible comprobar si cada celda de la conexión está conforme al comportamiento definido. Una forma de implementar este algoritmo es mediante un mecanismo *leaky bucket*.

## 10. Gestión del tráfico

### Monitorización del tráfico. Algoritmo GCRA

Para monitorizar la PCR el algoritmo GCRA usa el parámetro de tráfico  $T=1/PCR$ , y un parámetro de tolerancia ( $\tau$ ) especificado por el operador de la red.



## 10. Gestión del tráfico

### Monitorización del tráfico. Algoritmo GCRA

- Para monitorizar la SCR el algoritmo GCRA usa el parámetro de tráfico  $T_s=1/SCR$ , y un parámetro de tolerancia de rafageo ( $\tau_s$ ) calculado como:

$$\tau_s = (MBS-1)(T_s-T)$$

Para monitorizar varios parámetros de tráfico a la vez, se concatenan GCRA

## 10. Gestión del tráfico

### Monitorización del tráfico. Algoritmo GCRA

▪ Cuando la red transporta la información de una determinada conexión, se suministra la calidad de servicio asignada a dicha conexión y se asegura mediante un GCRA, que las características del tráfico se ajustan a lo definido en la petición de la conexión. Para lograr este objetivo, son necesarios controles de vigilancia en la red que actúen sobre conexiones que no cumplan con lo establecido, adoptando las medidas oportunas.

▪ Esta vigilancia se realiza mediante el Usage Parameter Control (UPC) en la UNI, y opcionalmente es posible utilizar el Network Parameter Control en el NNI.

Las funciones CAC y UPC/NNC trabajan conjuntamente, protegiendo al sistema de congestión mientras que aseguran la calidad de servicio de las demás conexiones.

## 10. Gestión del tráfico

### Conformado del tráfico

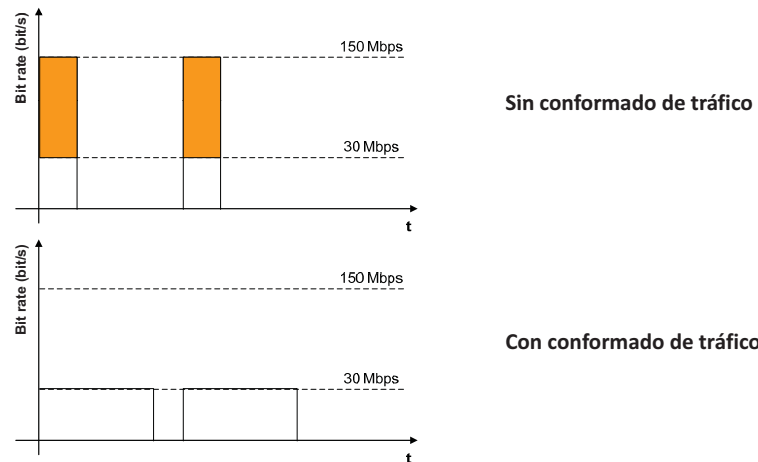
- La función de conformado del tráfico modifica el flujo de tráfico de celdas ATM, mejorando la eficiencia de la red, ya que elimina picos de tráfico y el jitter de celdas.
- Como resultado, tenemos un flujo más predecible y una mejor asignación de recursos.
- El conformado del tráfico puede realizarse a la entrada o a la salida del conmutador ATM.

Mientras que los controles de vigilancia del tráfico se preocupan de que las conexiones cumplan con lo contratado, el conformado del tráfico hace posible que algunas aplicaciones que podrían no funcionar, funcionen.



## 10. Gestión del tráfico

### Conformado del tráfico



## 10. Gestión del tráfico

### Algoritmo Leaky Bucket

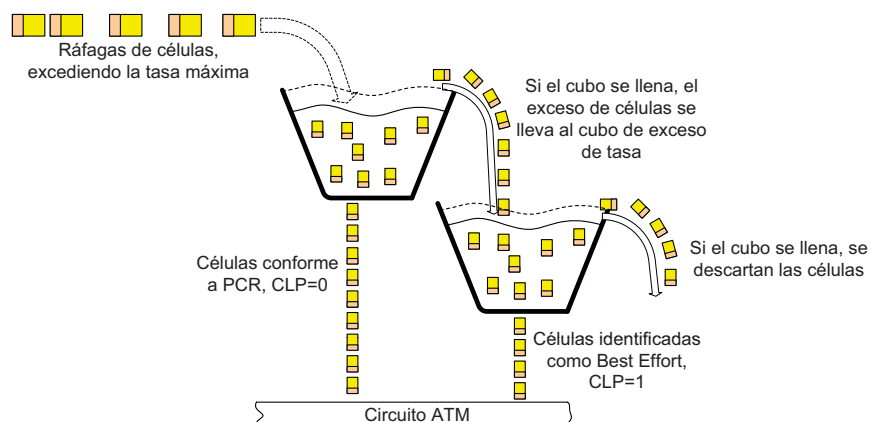
Las funciones UPC/NPC pueden utilizar varios algoritmos Leaky Bucket para vigilar cada conexión. El mecanismo Leaky Bucket utiliza dos parámetros:

- 1) Incremento de velocidad o de llenado del cubo (bucket)
- 2) Límite que define el tamaño del cubo

Quando se utilizan diferentes parámetros para describir el tráfico (i.e.: PCR y SCR) de una conexión, se utilizan múltiples leaky buckets en cascada.

## 10. Gestión del tráfico

### Algoritmo Leaky Bucket



## 10. Gestión del tráfico

### Gestión de colas a nivel de paquete

- En la red ATM, al dividirse los paquetes en celdas, si se pierde una celda es necesario retransmitir el paquete completo. Esto provoca un incremento considerable del tráfico y por tanto, la probabilidad de ocasionar situaciones de congestión es mayor.
- Para solventar este problema, se utilizan dos mecanismos denominados Early Packet Discard (EPD) y Partial Packet Discard (PPD). Estos mecanismos se aplican al tráfico ABR y UBR que utilizan conexiones de clase AAL5.
- Utilizando estos mecanismos y ante una situación de congestión, las celdas se descartan a nivel de paquete, no a nivel de celda, reduciendo drásticamente las retransmisiones de paquetes.

## 10. Gestión del tráfico

### ▪ Gestión de colas a nivel de paquete

1) **Early Packet Discard (EPD)**. Cuando se produce congestión y las colas se llenan, el método EPD descarta las celdas pertenecientes a los nuevos paquetes que llegan a la cola. De esta forma, queda espacio libre para las celdas de paquetes que ya tienen alguna encolada.

2) **Partial Packet Discard (PPD)**. Si el método EPD no consigue evitar la congestión y se siguen perdiendo celdas, se puede aplicar el método PPD. En PPD, en el momento en que se pierde una celda de un paquete, se descartan todas las celdas siguientes asociadas a dicho paquete.

Los métodos EPD y PPD se complementan el uno con el otro de forma efectiva, consiguiendo mejorar la llegada completa de paquetes en situaciones de congestión. El EPD aumenta la probabilidad de que los paquetes encolados abandonen el conmutador sin problemas y el PPD minimiza el número de paquetes que pueden llegar a ser invalidados en la cola.

## 11. Señalización en ATM

### ▪ ¿ Por qué es necesaria la señalización en ATM ?

ATM es un protocolo de comunicación por conmutación de circuitos: Es necesario establecer un circuito virtual antes de transmitir información de usuario.

▪ Los usuarios de la red que utilizan Circuitos Virtuales Conmutados (SVC) tienen que utilizar un procedimiento de señalización para establecer la conexión entre ellos, de forma análoga al procedimiento de establecimiento de llamada en la red telefónica.

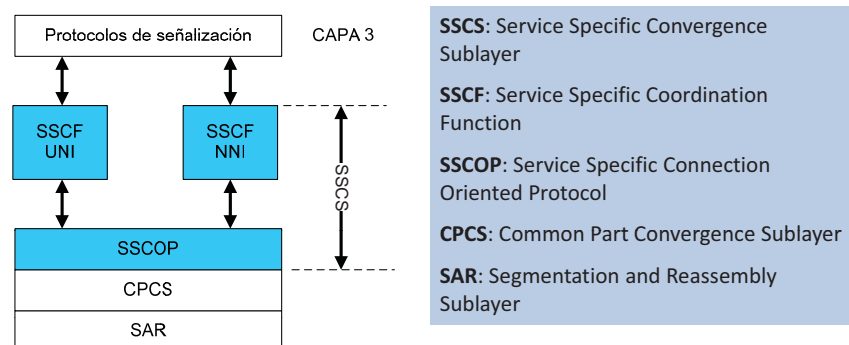
▪ En ATM, la información de señalización se envía por un canal separado, concretamente todas las celdas enviadas por VCI-5 son reconocidas por el conmutador como celdas de señalización.

▪ Se utiliza una capa AAL de adaptación especial (SAAL) para empaquetar la información de señalización (AAL5).

## 11. Señalización en ATM

### ▪ Transmisión de la señalización en ATM

La información de señalización debe transmitirse libre de errores y para ello se define un protocolo específico. Para ello, se definen una arquitectura específica dentro de la capa de adaptación AAL5.



## 11. Señalización en ATM

### ▪ Transmisión de la señalización en ATM

▪ La capa SSCS (Service Specific Convergence Sublayer) está compuesta de dos subcapas:

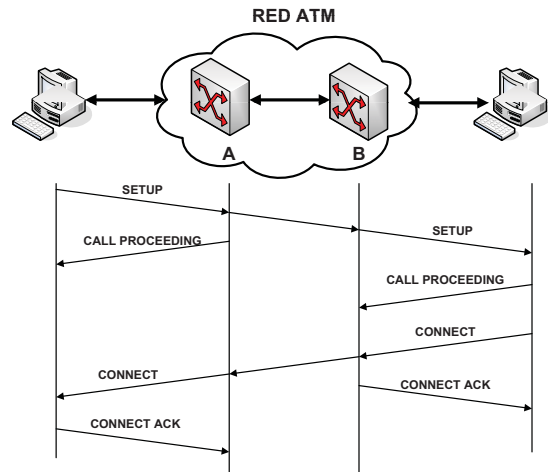
1. **SSCF: Service Specific Coordination Function**, que actúa como interfaz entre la SSCOP y las capas superiores

2. **SSCOP: Service Specific Connection Oriented Protocol**, protege la información frente a errores, de forma similar al protocolo HDLC.

▪ La señalización en ATM se realiza mediante un conjunto predefinido de mensajes que se intercambian entre un terminal ATM y un conmutador o entre dos conmutadores.

# 11. Señalización en ATM

## ▪ Ejemplo de señalización UNI



## Tema 4

### Conmutación de Etiquetas MPLS

1

## Tema 4

### Conmutación de Etiquetas (MPLS)

2

### Visión global

**IP** es conmutación de paquetes no orientada a la conexión (datagramas).

- **MPLS** introduce una estructura orientada a conexión en redes IPv4, permitiendo
  - QoS
  - Ingeniería de tráfico

3

### Contenidos

- 4.1. Conmutación IP.
- 4.2. Concepto de conmutación de etiquetas.
- 4.3. Cabecera MPLS
- 4.4. Asignación y eliminación de las etiquetas
- 4.5. Distribución de etiquetas
- 4.6. Ingeniería de tráfico
- 4.7. Redes privadas virtuales con VPN

4

## 4.1. Conmutación IP

### Direcciones IP

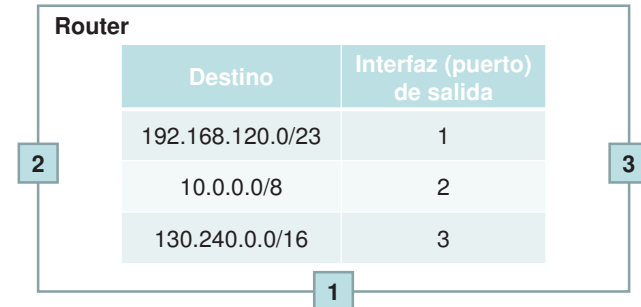
- Todos los datagramas IP llevan en su cabecera su dirección destino. Dicha dirección es de 32 bits y suele expresarse en notación “punto decimal”, escribiendo cada byte como el decimal equivalente:  
Ej: 192.168.120.67
- La dirección IP se divide una dirección de red (prefijo) y una dirección de host (sufijo).
- Para diferenciar la dirección de red del sufijo se emplea una máscara de 32 bits que tiene a 1 los bits que son de la dirección de red.  
Ej: Dirección IP 192.168.120.67 con Máscara 255.255.254.0  
9 bits para el sufijo y  $32-9=23$ bits para la dirección de red.  
Dirección de la red 192.168.120.0
- Notación CIDR: Dirección IP / N° bits que corresponden a la red.  
192.168.120.0/23

5

## 4.1. Conmutación IP

### Enrutamiento

- Cada enrutador tiene una tabla de enrutamiento.
- El encaminamiento se realiza en base al prefijo (más largo) que encaja.

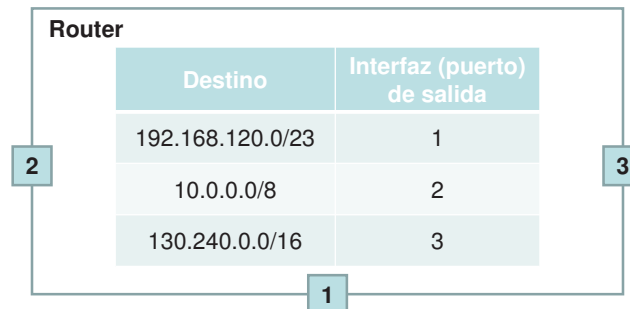


- Ej: ¿A dónde va 192.168.121.5?

6

## 4.1. Conmutación IP

### Enrutamiento



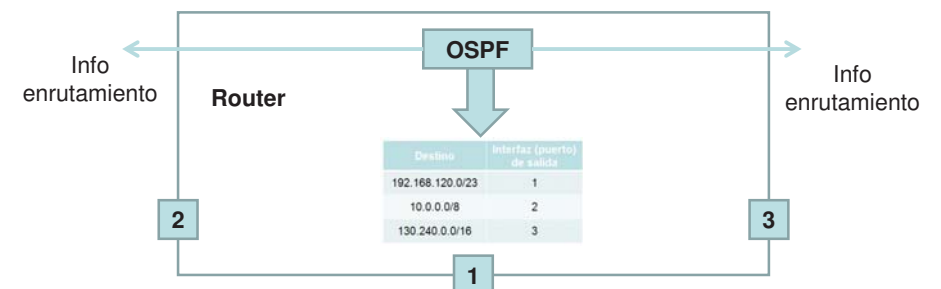
- Todas las direcciones con el mismo prefijo constituyen una **clase equivalente de encaminamiento** (*FEC – Forwarding Equivalent Class*).

7

## 4.1. Conmutación IP

### Protocolo de enrutamiento

- Los protocolos de encaminamiento (p.e. OSPF) construyen las tablas de encaminamiento, intercambiando información con otros enrutadores.



- Hay dos funcionalidades distintas:
  - construir las tablas de encaminamiento.
  - Realizar el re-envío de los datagramas.

8

## 4.1. Conmutación IP

### Inconvenientes

- Tablas de encaminamiento grandes. La búsqueda del prefijo consume bastantes recursos hardware. Esencialmente resuelto con nuevos algoritmos y hardware específico.
- No se puede ofrecer QoS (para el enrutador todos los datagramas que llegan son iguales).
- No se puede hacer ingeniería de tráfico (determinar por qué camino van a ir ciertos paquetes).
- Los puntos anteriores se pueden resolver con IP sobre ATM, pero esto requiere administrar esencialmente dos redes.

9

## 4.1. Conmutación IP

### Hacia MPLS

Se trata de:

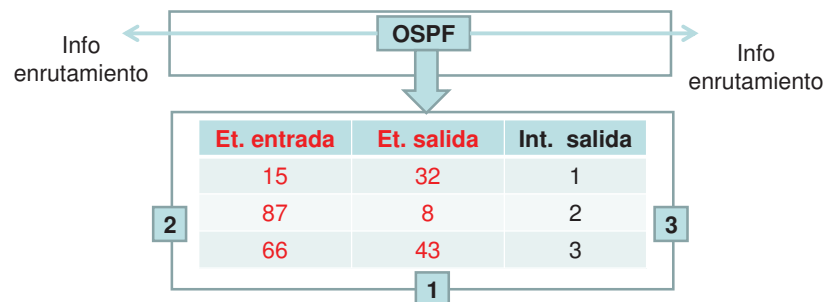
- Conseguir que los datagramas IP viajen por la red de manera independiente.
- Sin embargo, lo habitual es que las condiciones de red (y por tanto las tablas de enrutamiento) no cambien a la escala de tiempo de los datagramas, de modo que muchas datagramas acaban viajando por el mismo camino.
- **Separar** las funcionalidades de la construcción de las tablas de encaminamiento y de re-envío.

10

## 4.2. Concepto de MPLS

### Concepto de MPLS

- La idea inicial de MPLS consiste en asignar una etiqueta (label) a cada FEC, y realizar la conmutación en base a las etiquetas.
- Los equipos que funcionan con este esquema se denominan **Label Switching Routers (LSR): integran MPLS e IP**



¿Diferencia con IP sobre ATM?

11

## 4.2. Concepto de MPLS

### Concepto de MPLS

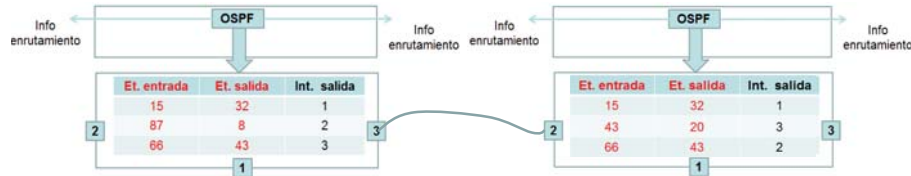
- El funcionamiento de las etiquetas es análogo al los VCI/VPI de ATM:
  - Las etiquetas sólo tienen significado local.
  - Cuando llega un paquete con una etiqueta, se extrae de la tabla la interfaz de salida y la nueva etiqueta que debe llevar.
  - Una conexión se establece gracias a una cadena de etiquetas de entrada/salida entre varios LSR.
  - **Pero:**
    - las conexiones son **unidireccionales!**
    - las conexiones sólo se distinguen por etiquetas y no por el interfaz (puerto) de entrada.
- Etiquetas locales: las tablas mucho más pequeñas.
- Gracias a que se pueden diferenciar flujos mediante las etiquetas se pueden establecer mecanismos de QoS e ingeniería de tráfico.

12

## 4.2. Concepto de MPLS

### Concepto de MPLS

- El camino que sigue un paquete a través de una red MPLS se denomina “camino conmutado por etiquetas” (**LSP** – Label switched path).
- Las tablas de encaminamiento de etiquetas se denominan “label forward information base (**LFIB**)”.
- El protocolo encargado de la distribución de las etiquetas es **LDP**.



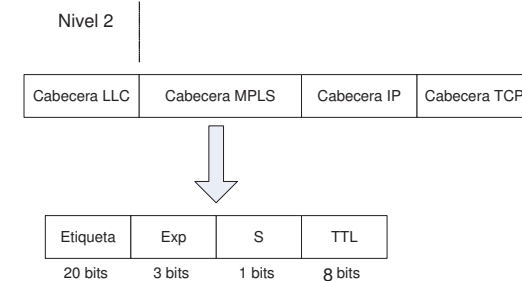
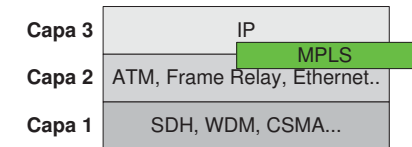
¿Cómo viaja la info de enrutamiento?

13

## 4.3. Cabecera MPLS

### Posición OSI

- La funcionalidad de MPLS está entre los niveles OSI 2 y 3.
- La cabecera MPLS se añade entre la cabecera IP y el nivel de “enlace”:



14

## 4.3. Cabecera MPLS

### Campos

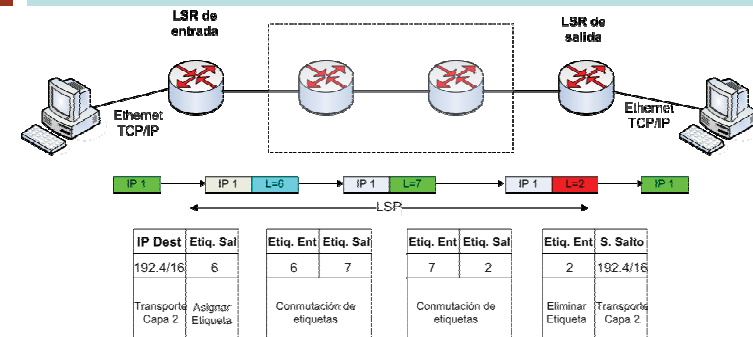
Etiqueta	Exp	S	TTL
20 bits	3 bits	1 bits	8 bits

- Etiqueta: 20 bits para la etiqueta MPLS
- EXP: 3 bits para identificar la clase de servicio
- S: 1 bit de stack para poder apilar etiquetas de forma
  - S=0 indica que siguen más hay etiquetas apiladas
  - S=1 indica que se trata de la última etiqueta.
- TTL: 8 bits para time to live, con la funcionalidad estándar TTL de las redes IP.

15

## 4.4. Asignación y eliminación

### Push & Pop



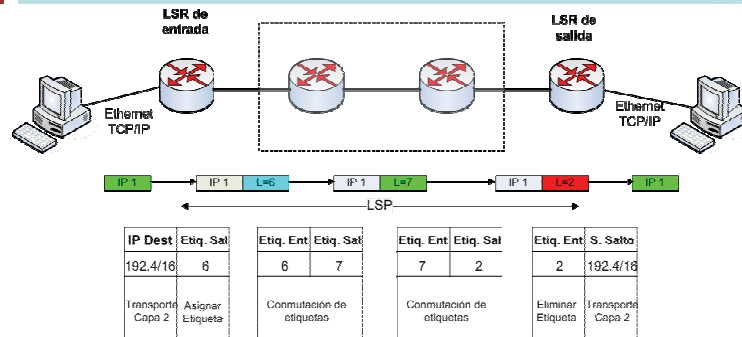
Cuando un paquete IP llega a una red MPLS:

- El LSR de entrada asigna una etiqueta (*push*)
- Los LSR intermedios realizan conmutación de etiquetas.
- El LSR de salida elimina la etiqueta (*pop*).

16

## 4.4. Asignación y eliminación

### Penultimate hop popping

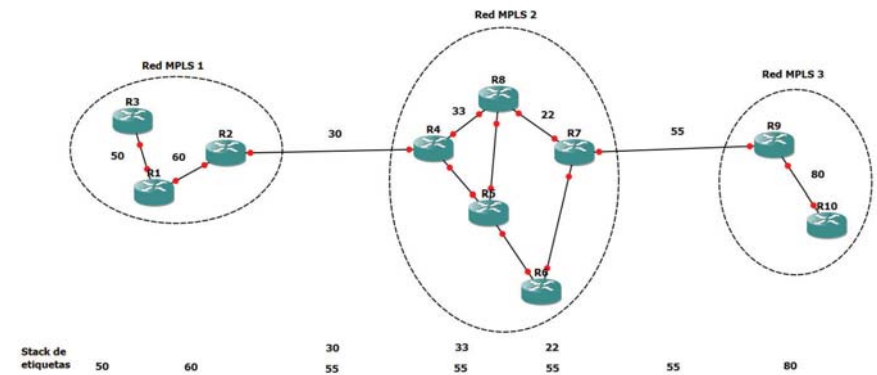


- El LSR de salida realmente no conmuta por etiqueta.
- La etiqueta se suele quitar en el penúltimo salto.
- A diferencia de ATM, los LSP son unidireccionales.

17

## 4.4. Asignación y eliminación

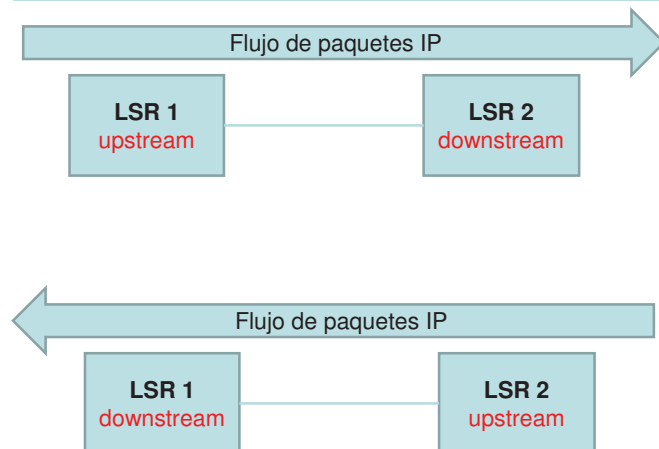
### Apilamiento de etiquetas



- Las etiquetas se pueden apilar al atravesar múltiples dominios.
  - Esto permite la formación de túneles.
- ¿Cuál sería la cabecera en la red?; ¿Cómo se establecería un segundo camino?*

## 4.5. Distribución de etiquetas

### Upstream & downstream



19

## 4.5. Distribución de etiquetas

### Esquemas de creación y distribución de etiquetas

Hay dos esquemas de creación de etiquetas:

- **Independiente:** Un LSR asigna una etiqueta a una FEC tan pronto como aparece en su tabla de enrutado.
- **Controlado:** Un LSR sólo asigna una etiqueta a una FEC cuando es el LSR de salida o cuando recibe una etiqueta de un LSR downstream.

También existen dos esquemas de distribución:

- **Downstream sin solicitud:** El LSR distribuye la etiqueta de entrada a sus vecinos sin que éstos la soliciten.
- **Downstream con solicitud (o bajo demanda).** Un LSR sólo manda su etiqueta de entrada cuando un LSR upstream se lo solicita.

20



## 4.5. Distribución de etiquetas

### Esquemas de creación y distribución de etiquetas

Los esquemas anteriores suelen combinarse como:

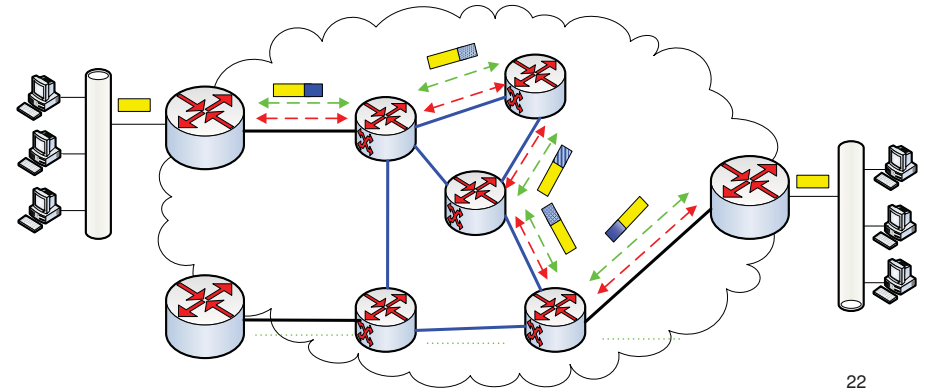
- **Creación independiente, downstream sin solicitud.**
  - Puede darse el caso de que un LSR (distinto al de salida) no disponga de etiqueta de salida.
- **Creación controlada, downstream con solicitud.**
  - Asegura que está establecido el LSP antes de que el LSR de entrada empiece a usarlo.

21

## 4.5. Distribución de etiquetas

### Esquemas de creación y distribución de etiquetas

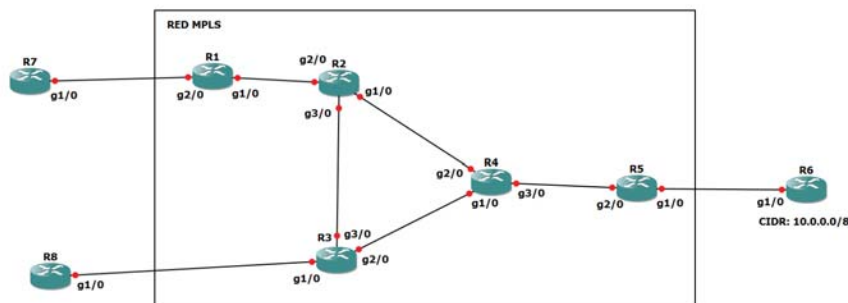
#### Asignación y Conmutación de etiquetas



22

## 4.5. Distribución de etiquetas

### Ejemplo: independiente, downstream sin solicitud (I)



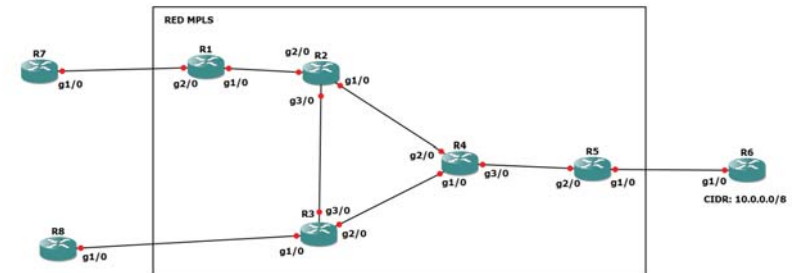
A la red MPLS se le conecta la nueva FEC 10.0.0/8. Suponemos que empieza a fluir tráfico IP desde R7 y R8 hasta R6.

1) Los LSR de la red MPLS identifican la FEC 10.0.0/8.

23

## 4.5. Distribución de etiquetas

### Ejemplo: independiente, downstream sin solicitud (II)



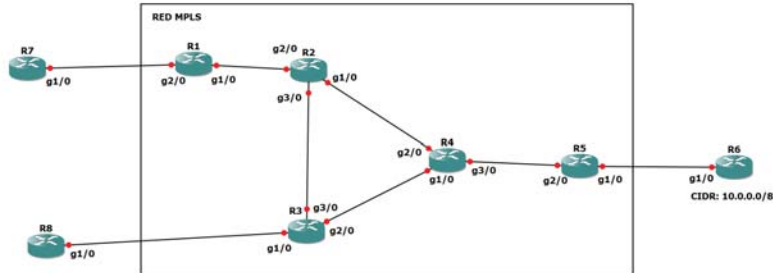
2) Cada LSR elige una **etiqueta de entrada para esta FEC.**

3) Cada LSR sabe cuál es el próximo salto (por OSPF).

LSR	Et. ent.	Et. sal.	Sig. LSR	Int. sal
R1	--		R2	g1/0
R2	88		R4	g1/0
R3	--		R4	g2/0
R4	65		R5	g3/0
R5	101		R6	g1/0

## 4.5. Distribución de etiquetas

Ejemplo: independiente, downstream sin solicitud (III)

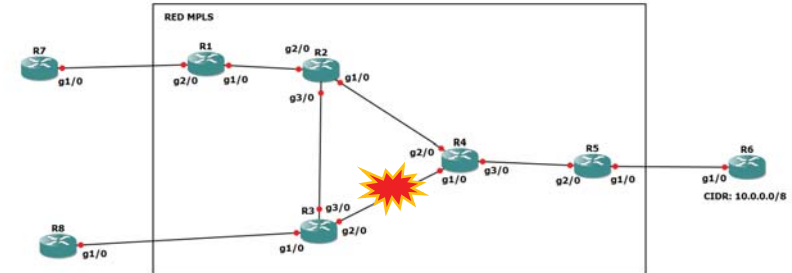


- 4) Cada LSR manda la etiqueta a todos sus vecinos.
- 5) Los vecinos *upstream* guardan la etiqueta recibida como etiqueta de salida.

LSR	Et. ent.	Et. sal.	Sig. LSR	Int. sal
R1	--	88	R2	g1/0
R2	88	65	R4	g1/0
R3	--	65	R4	g2/0
R4	65	101	R5	g3/0
R5	101	--	R6	g1/0

## 4.5. Distribución de etiquetas

Ejemplo: independiente, downstream sin solicitud (III)

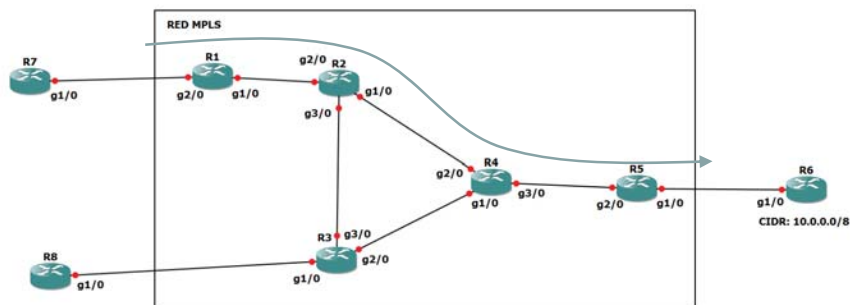


¿Qué ocurre si se cae el enlace entre R3 y R4?

LSR	Et. ent.	Et. sal.	Sig. LSR	Int. sal
R1	--		R2	g1/0
R2	88		R4	g1/0
R3	--		R4	g2/0
R4	65		R5	g3/0
R5	101		R6	g1/0

## 4.5. Distribución de etiquetas

Ejemplo: controlado, downstream con solicitud (I)



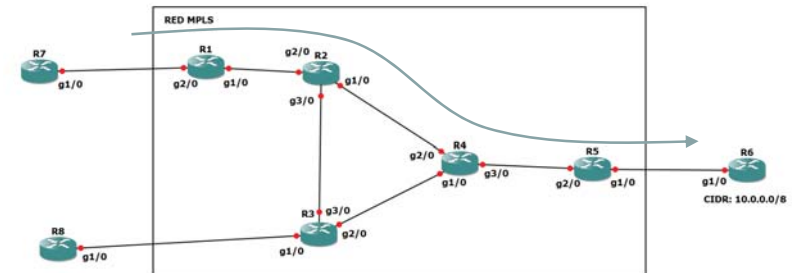
A la red MPLS se le conecta la nueva FEC 10.0.0.0/8. Suponemos que empieza a fluir tráfico IP desde R7 y R8 hasta R6.

- 1) Los LSR de la red MPLS identifican la FEC 10.0.0.0/8.

27

## 4.5. Distribución de etiquetas

Ejemplo: controlado, downstream con solicitud (II)

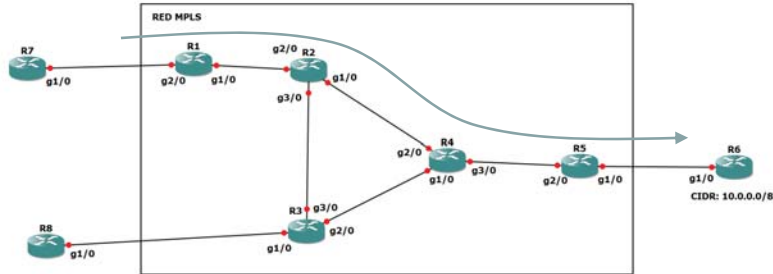


- 2) R1 no dispone de etiqueta de salida → se la pide a R2.
- 3) R2 pide una etiqueta a R4.
- 4) R4 la pide a R5.

LSR	Et. ent.	Et. sal.	Sig. LSR	Int. sal
R1			R2	g1/0
R2			R4	g1/0
R3			R4	g2/0
R4			R5	g3/0
R5			R6	g1/0

## 4.5. Distribución de etiquetas

Ejemplo: controlado, downstream con solicitud (III)

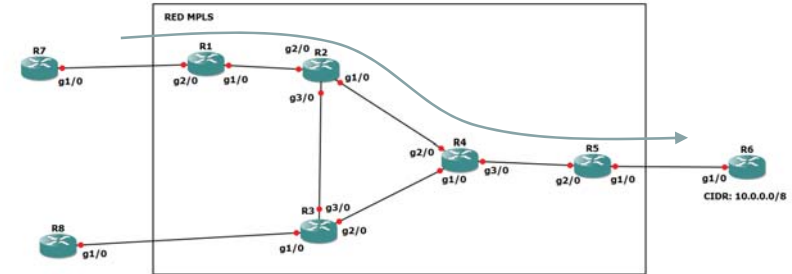


5) R5 es el LSR de salida, de modo que crea su etiqueta de entrada, y la pasa a R4.

LSR	Et. ent.	Et. sal.	Sig. LSR	Int. sal
R1			R2	g1/0
R2			R4	g1/0
R3			R4	g2/0
R4		101	R5	g3/0
R5	101	--	R6	g1/0

## 4.5. Distribución de etiquetas

Ejemplo: controlado, downstream con solicitud (IV)



6) R4 ya tiene etiqueta de salida, de modo que crea la suya de entrada y la pasa a R2.  
7) R2 crea la suya y la pasa a R1.

LSR	Et. ent.	Et. sal.	Sig. LSR	Int. sal
R1	--	88	R2	g1/0
R2	88	65	R4	g1/0
R3	--	--	R4	g2/0
R4	65	101	R5	g3/0
R5	101	--	R6	g1/0

## 4.5. Distribución de etiquetas

### LDP

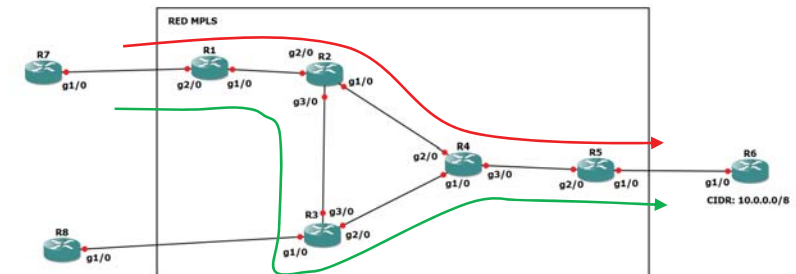
- El protocolo usado para distribuir las etiquetas se denomina **Label Distribution Protocol (LDP)**.
- LDP se basa en el encaminamiento hop-by-hop de OSPF, por lo que **no** permite ingeniería de tráfico.
- Emplea el esquema downstream sin solicitud (con creación independiente o controlada).
- LDP emplea cuatro tipos de mensajes:
  - Descubrimiento: detectar la presencia de otros LSR
  - Sesión: establece una conexión entre LSR para que puedan empezar a negociar etiquetas.
  - Anuncios: gestión de etiquetas
  - Notificación: avisos sobre errores.

Sobre UDP

Sobre TCP

## 4.6. Ingeniería de tráfico

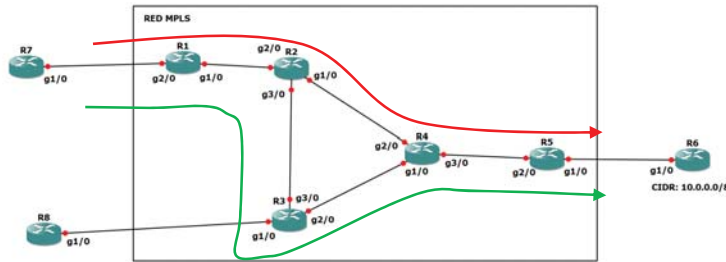
### Concepto



- La ruta más corta (menos saltos) no siempre es la mejor (congestión, mantenimiento de enlaces, distribución de carga...)
- Ingeniería de tráfico: adaptar los flujos a los recursos físicos de la red
- El LSR de entrada elige la ruta. Una vez elegida, es necesario especificarle a la red explícitamente la ruta a seguir → **Enrutamiento explícito**.

## 4.6. Ingeniería de tráfico

### Concepto



- En IP el encaminamiento por defecto es hop-by-hop (cada router decide). Si bien el encaminamiento explícito es posible, produce mucho overhead (las direcciones de todos los saltos tienen que ir en cada paquete).
- En MPLS una vez establecido el LSP, no hay overhead.
- Un LSP para ingeniería de tráfico se denomina túnel y es unidireccional.

33

## 4.6. Ingeniería de tráfico

### RSVP-TE

Para establecer un túnel:

- OSPF proporciona info sobre el estado de todos los enlaces.
- El LSR de entrada usa esa info para calcular un camino a través de la red que satisfaga los requerimientos de ancho de banda.
- RSVP-TE (Resource Reservation protocol – traffic engineering) establece el túnel con creación de etiquetas ordenada, y distribución bajo demanda.
- RSVP-TE no es compatible con LDP, se usa uno u otro.

34

## 4.7. MPLS VPN

### Introducción

VPN: Emular una red **privada** sobre una infraestructura común. Las oficinas operan con IP.



35

## 4.7. MPLS VPN

### Introducción

Hay dos mecanismos para establecer una VPN:

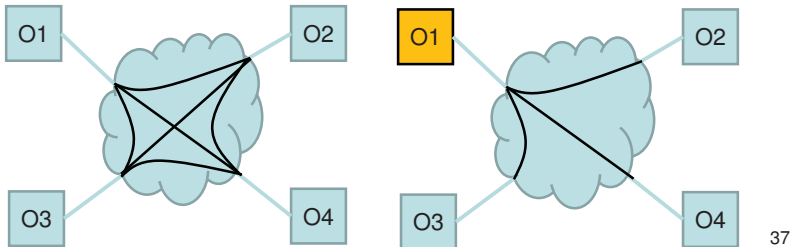
- **Modelo Overlay:** la red compartida se usa a **nivel de enlace** (OSI capa 2), proporcionando conexiones punto a punto entre las oficinas (p.e. PVCs ATM).
- **Modelo Peer-to-Peer:** la red compartida se usa a **nivel de red** (OSI capa 3) y realiza conmutación del tráfico procedente de las oficinas.

36

## 4.7. MPLS VPN

### Overlay

- Modelo Overlay: el más empleado hasta la introducción de MPLS, ya que garantiza la privacidad.
- La conectividad se establece mediante:
  - Conexión de todos con todos (fully meshed)
  - Oficina maestra

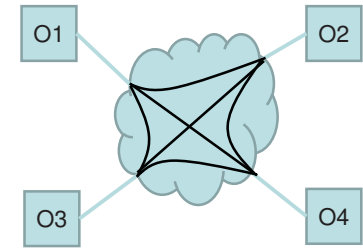


37

## 4.7. MPLS VPN

### Overlay – fully meshed

- Necesita  $N \times (N-1)/2$  enlaces.
- No es escalable.

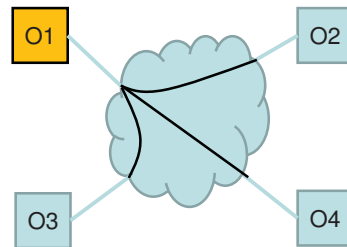


38

## 4.7. MPLS VPN

### Overlay – oficina maestra

- O1 es la encargada de redirigir el tráfico.
- Sólo necesita  $N-1$  enlaces.
- Más complejidad en O1.
- El tráfico pasa dos veces por la red (por ejemplo para ir de O3 a O2).

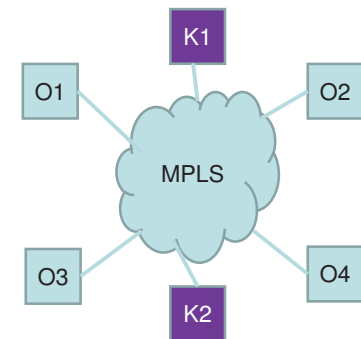


39

## 4.7. MPLS VPN

### Peer-to-peer

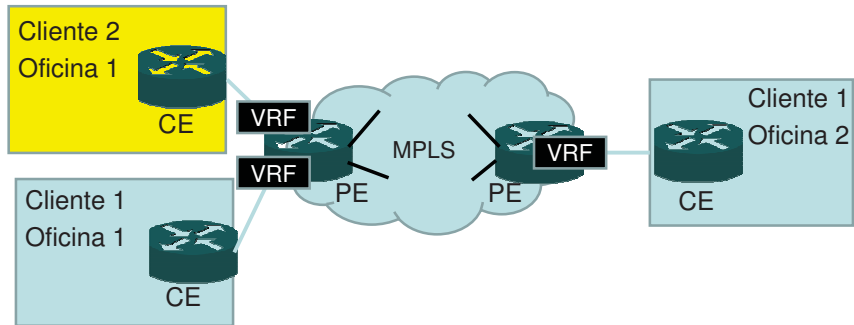
- La red conmuta el tráfico de las oficinas. Los enrutadores de las oficinas y de la red son pares (peers) a nivel IP
- Sólo requiere la conexión a la red.
- La info sólo pasa una vez por la red.
- Para ello la red tiene que conocer las tablas de enrutamiento de las oficinas.



40

## 4.7. MPLS VPN

### Peer-to-peer con MPLS

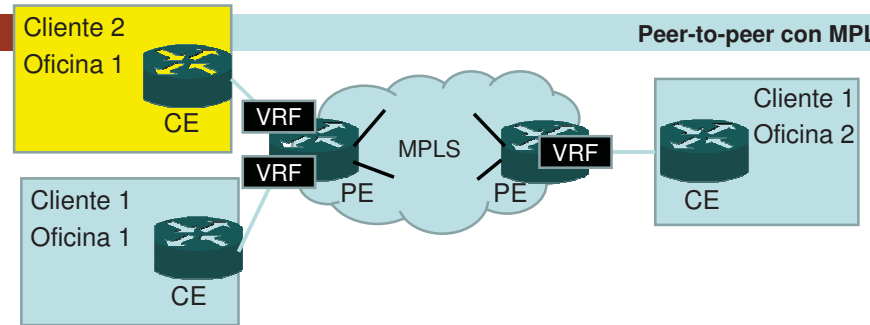


- Enrutadores del cliente conectados a la red: **client edge router** (CE).
- Enrutadores de la red conectados al cliente: **provider edge router** (PE).
- Los CE y PE se ven a nivel IP (son pares o *peers*).

41

## 4.7. MPLS VPN

### Peer-to-peer con MPLS



En los PE se implementa **Virtual Routing and Forwarding** (VRF).

- Cada cliente conectado a una interfaz.
- Cada interfaz tiene tabla IP y LFIB independiente → privacidad.
  - Cliente 1 y Cliente 2 pueden usar IPs iguales.
- Red MPLS: nunca mira las cabeceras del cliente → privacidad

42