

1. INTRODUCCIÓN A LAS REDES DE COMUNICACIONES

Sistema: elemento con una dirección individual y única dentro de una red capaz de comunicarse con otros sistemas de la red mediante un conjunto de protocolos

- ❖ **Finales:** generan y reciben información.
- ❖ **Intermedios:** encamina la información.

Red: medio común de comunicación y compartición de recursos. Debe haber un método para identificar cada dispositivo conectado: dirección de red.

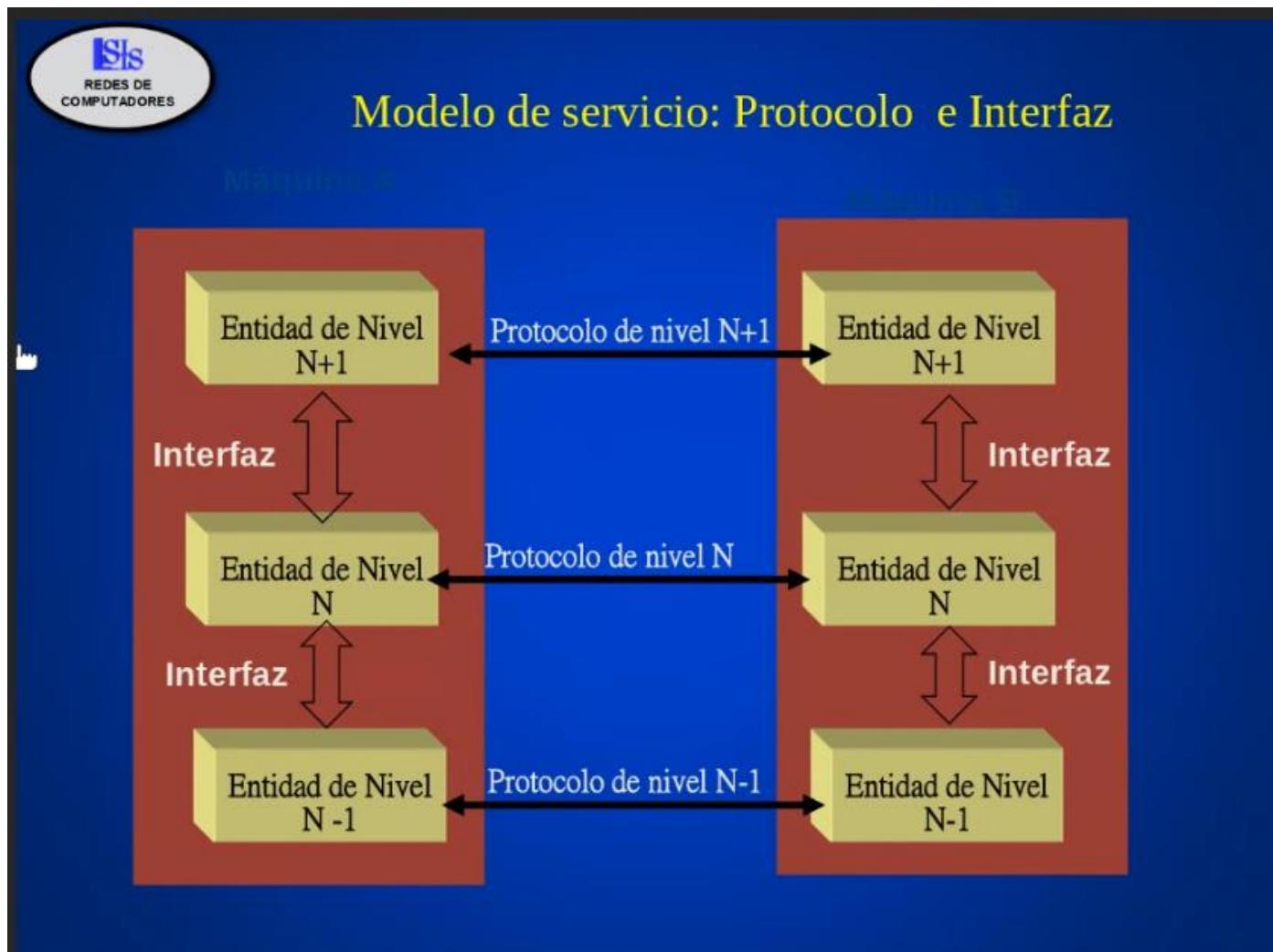
- ❖ **Redes de comunicaciones (o físicas):** formadas por la conexión directa de los equipos de usuario. Ej.: red de cable Ethernet, red inalámbrica WiFi.
- ❖ **Redes de computadoras (o abstractas):** formadas por la interconexión de redes de comunicaciones.
 - **Internet:** red de computadores con tecnología TCP/IP y formato IP de direccionamiento común.

Arquitectura estructurada de comunicaciones: conjunto de protocolos de comunicaciones que se ejecutan independientemente en diferentes niveles, exceptuando el nivel más elemental, el físico o de hardware.

Estratificación en niveles: reduce la complejidad de desarrollo. Favorece la labor de diseño. Si hay que realizar algún cambio en algún nivel no afecta a los demás.

Protocolo: conjunto de reglas que controlan la interacción entre sistemas.

Interfaz: conjunto de reglas de interacción entre entidades de niveles contiguos en el mismo sistema.

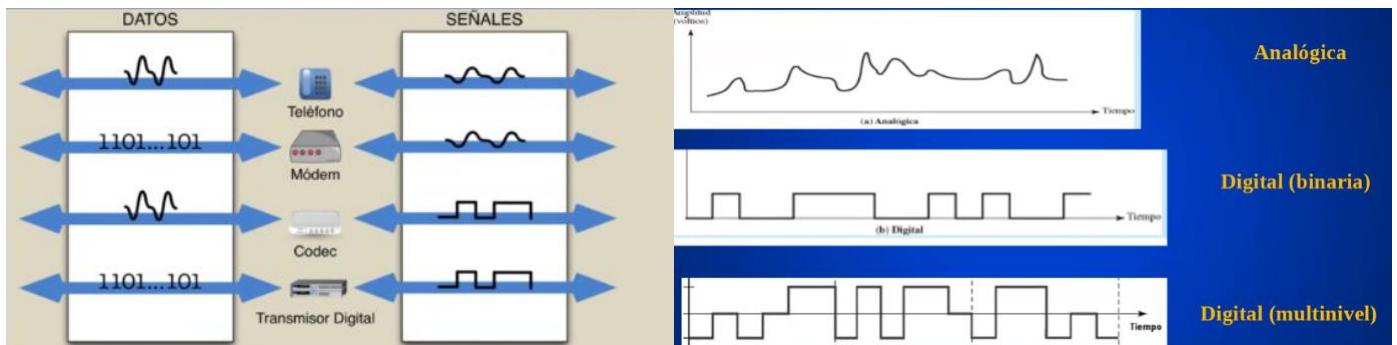


1.1 CONCEPTOS BÁSICOS DE TRANSMISIÓN DE DATOS

Datos analógicos: toman valores en un intervalo continuo

Datos digitales: toman valores discretos, como 0 y 1

Se transmiten mediante un **equipo terminal del circuito de datos** que adapta la naturaleza del dato al medio de transmisión



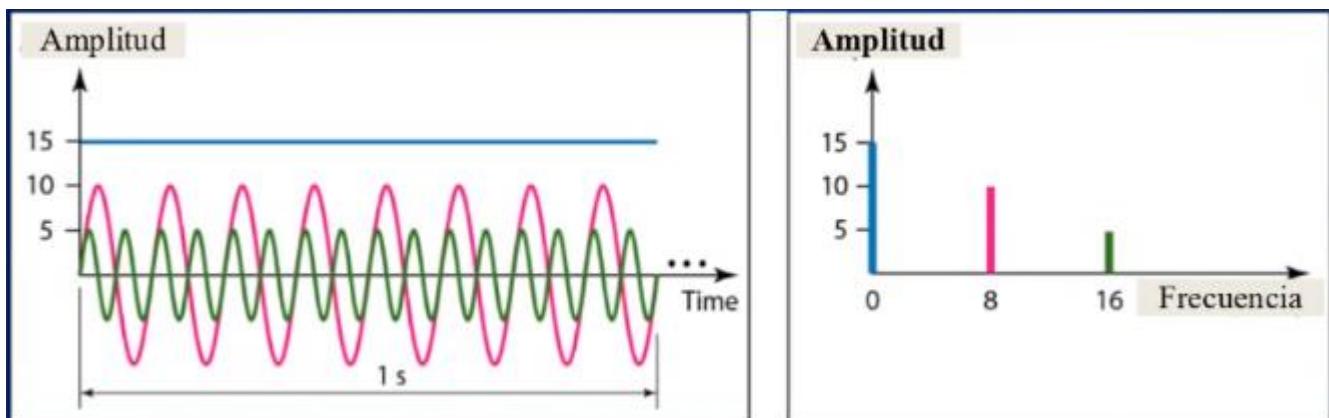
Periodo: tiempo entre dos puntos equivalentes

Frecuencia: inverso del periodo

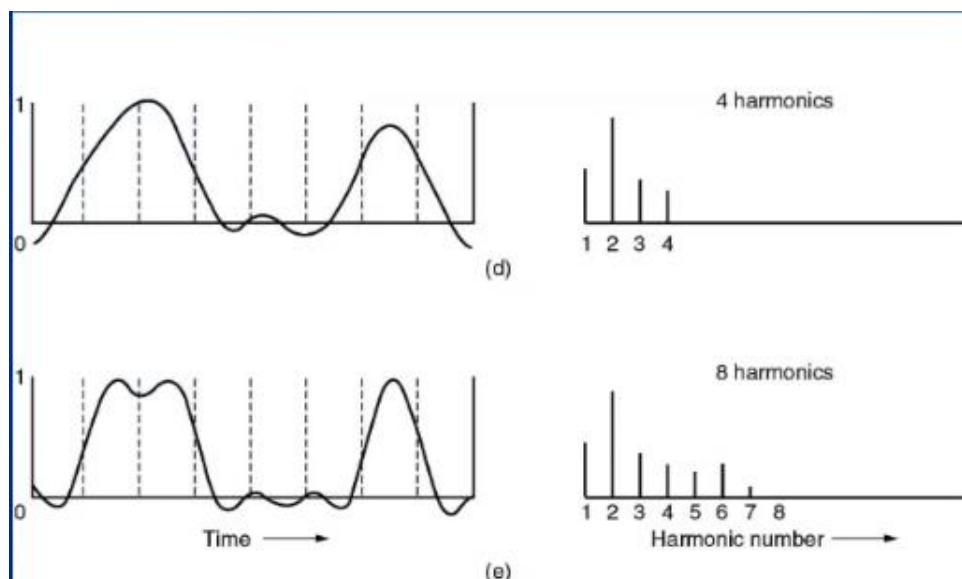
Amplitud: valor de pico

Fase: posición de la onda respecto a $t=0$

Una sola señal simple (o seno) no transmite datos. Para transmitir datos hace falta una señal compuesta, formada por múltiples ondas seno.



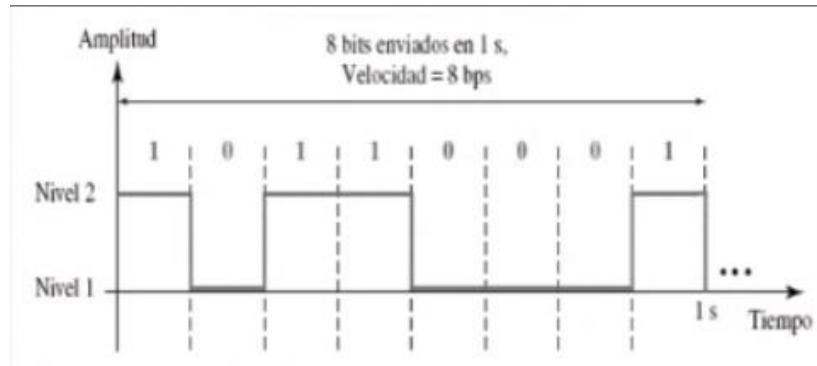
Ancho de banda: rango de frecuencias por el cual se transmite la información. Cuanto mayor es el ancho de banda mejor se reconstruye la señal en el destino.



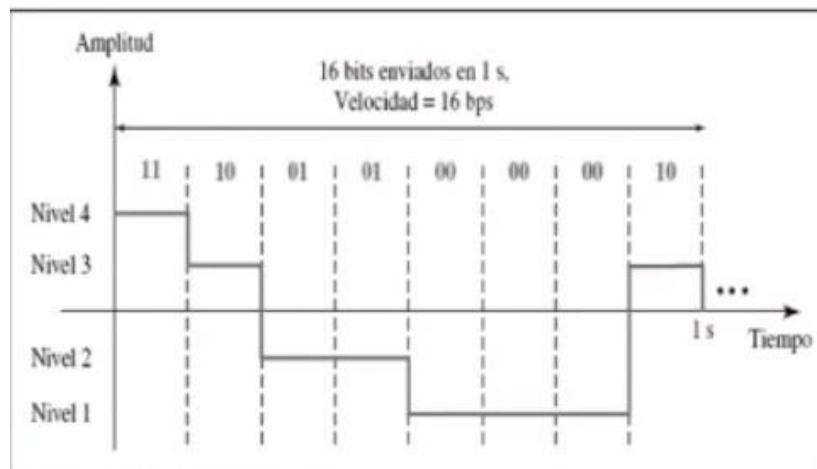
Velocidad de transmisión: número de bits por segundo. Es igual a $1/T$, siendo T la duración de 1 bit

Velocidad de señalización: número de elementos de señalización por segundo. Es igual a $1/T_s$, siendo T_s la duración de un intervalo de señal. Se mide en Baudios. Un elemento de señalización puede transmitir uno o más bits, según el número de estados posibles (niveles) de señalización (N).

$$v_{bps} = v_{baudios} * \log_2 N$$



a. Una señal digital con dos niveles



b. Una señal digital con cuatro niveles

Transmisión simplex: la información se transmite solo en un sentido.

Transmisión semidúplex: la información se transmite en ambos sentidos, pero no a la vez.

Transmisión dúplex: la información se transmite en ambos sentidos a la vez.

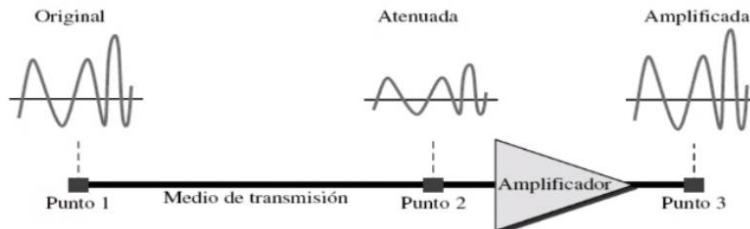
1.2 MEDIOS DE TRANSMISIÓN Y CAPACIDAD DE CANAL

Medios guiados: establecen un camino físico entre la fuente y el destino. Ej.: par trenzado, cable coaxial, fibra óptica

Medios no guiados: medios inalámbricos.

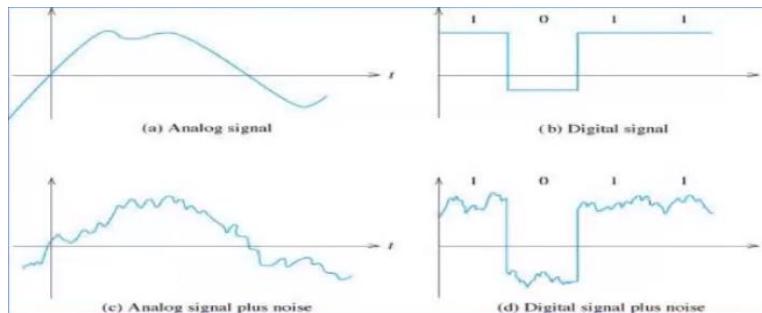
Atenuación: perdida de potencia de la señal entre dos puntos. Incrementa con la distancia. Se mide en decibelios.

$$\alpha = 10 \log_{10} \frac{P_2}{P_1} \text{ dB}$$



Ruido: señales no deseadas que se combinan con la señal transmitida haciendo que la señal recibida sea distinta a la que se ha enviado. Se mide en decibelios.

$$\frac{S}{R} = 10 \log_{10} \frac{P_{Señal}}{P_{Ruido}} \text{ dB}$$



SEÑAL ANALÓGICA	SEÑAL DIGITAL
La atenuación se corrige con amplificadores	La atenuación se corrige con regeneradores
No es reconstruible porque también amplifica el ruido	Se puede reconstruir.
Siempre se añade ruido	No se añade ruido

Capacidad de un canal: máxima velocidad de transmisión de datos. Influyen el ancho de banda (W) y la calidad del canal (C).

Teorema de Nyquist: define la máxima velocidad de transmisión para canales sin ruido, cuya única limitación es el ancho de banda.

$$C = 2W \text{ baudios}$$

$$C = 2W \log_2 N \text{ bits/s}$$

Teorema de Shannon: define la máxima capacidad de un canal en función del ancho de banda y de la relación señal/ruido que determina el número de niveles que puede tomar una señal.

$$N = \sqrt{1 + \frac{P_{Señal}}{P_{Ruido}}} \text{ niveles}$$

$$C = W \log_2 \left(1 + \frac{P_{Señal}}{P_{Ruido}} \right) \text{ bits/s}$$

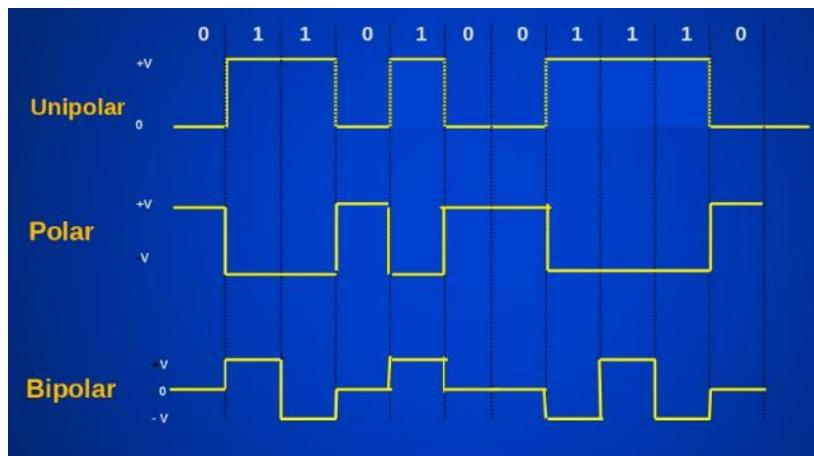
1.3 TÉCNICAS DE TRANSMISIÓN

Transmisión digital: las señales representan la información como pulsos de voltaje.

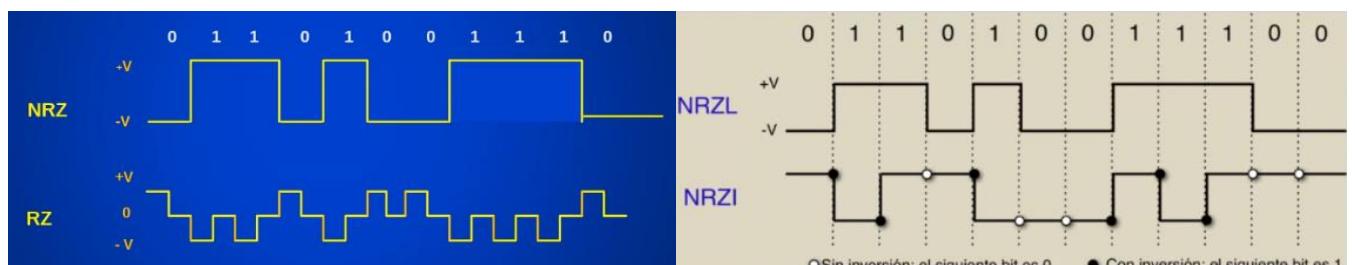
Transmisión analógica: las señales representan la información como variaciones continuas de voltaje.

Datos digitales/Señal digital:

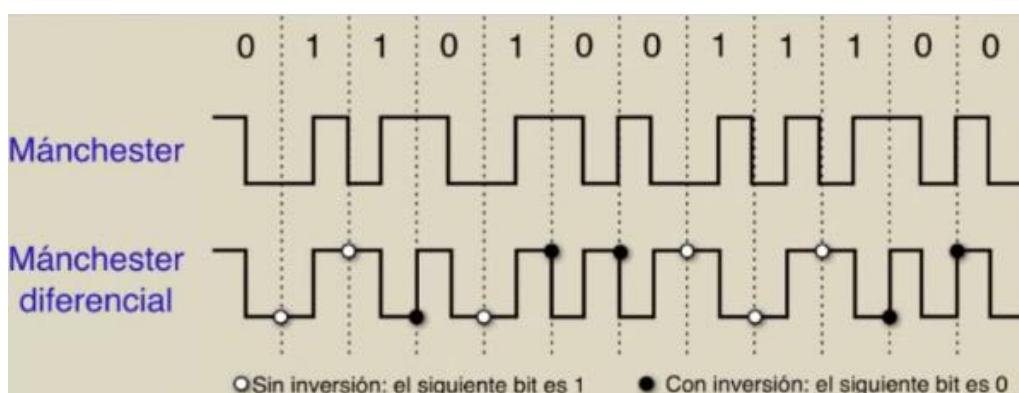
- ❖ **Unipolar:** la señal toma valor 0 o positivo.
- ❖ **Polar:** la señal toma valor positivo o negativo.
- ❖ **Bipolar:** la señal toma valor positivo, negativo o 0.



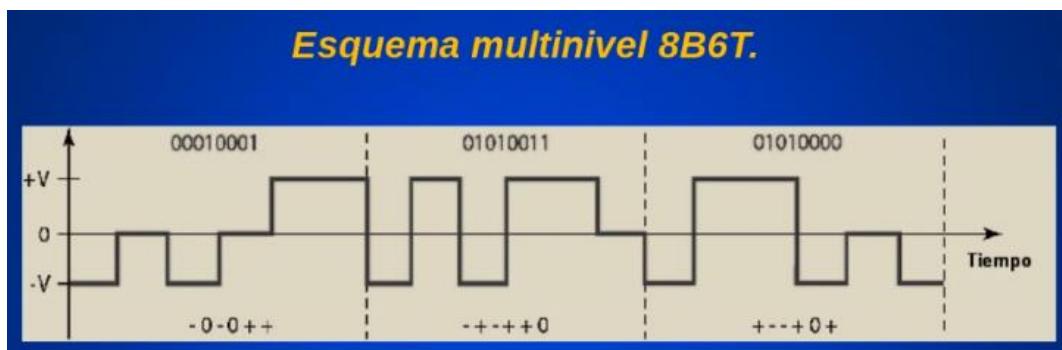
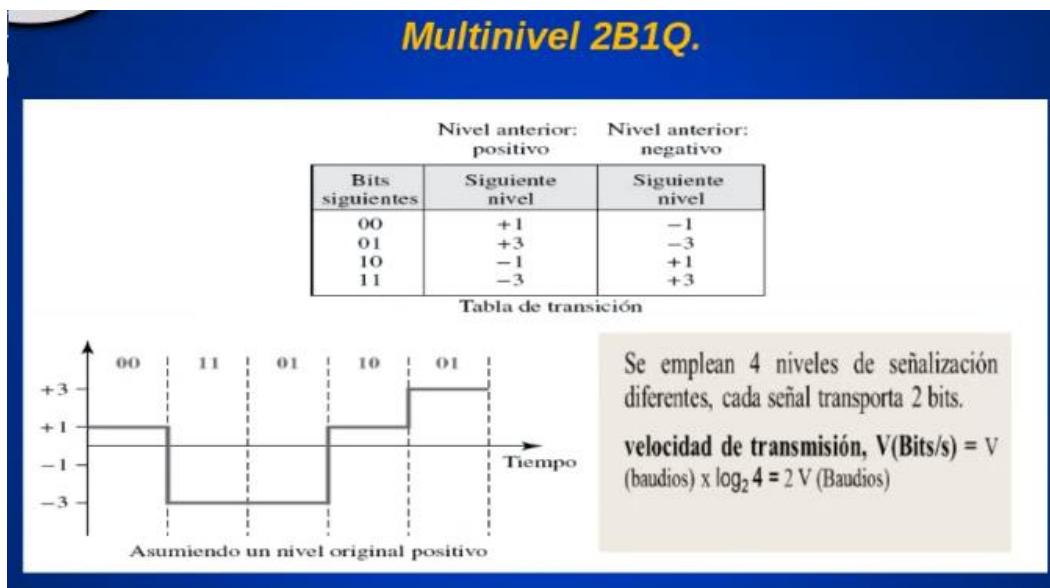
- ❖ **NRZ (no retorno a cero):** la señal no retorna a cero en la mitad del bit. El destino no sabe cuándo empieza y acaba un bit, así que puede haber problemas de sincronización.
 - **NRZ-L:** el nivel de voltaje determina el valor del bit.
 - **NRZ-I:** la inversión (o falta de inversión) determina el valor del bit. Soluciona el problema de sincronismo con bits a 1 pero no con bits a 0.
- ❖ **RZ (retorno a cero):** la señal retorna a cero en la mitad del bit. Al necesitar 2 baudios por bit son menos eficientes que los NRZ, ya que necesitan el doble de ancho de banda.



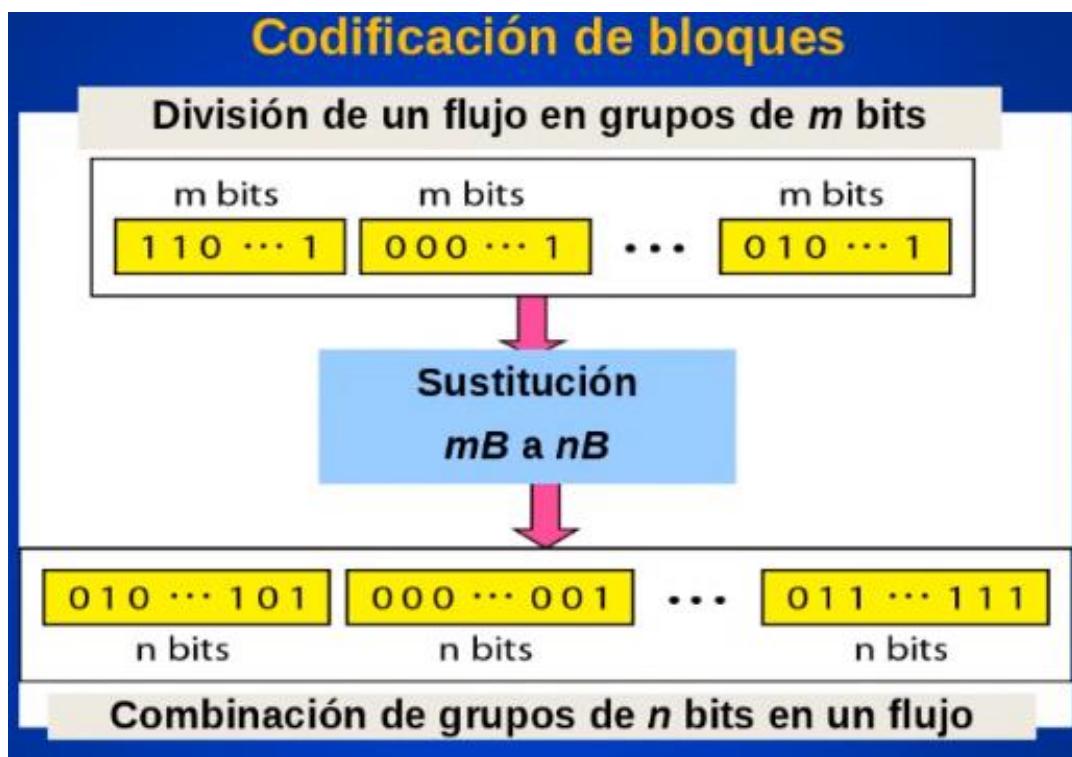
- ❖ **Manchester:** hay ruptura a mitad del intervalo. Se usan 2 baudios por bit. Sincroniza mediante la ruptura.
 - **Manchester diferencial:** utiliza inversión.



- ❖ **Multinivel:** un patrón de m elementos de datos se codifica como un patrón de n elementos de señal donde $2^m \leq L^n$. Se transmiten 2 bits por baudio. Cada formato multinivel se nombra mBn [nºvalores de señal].



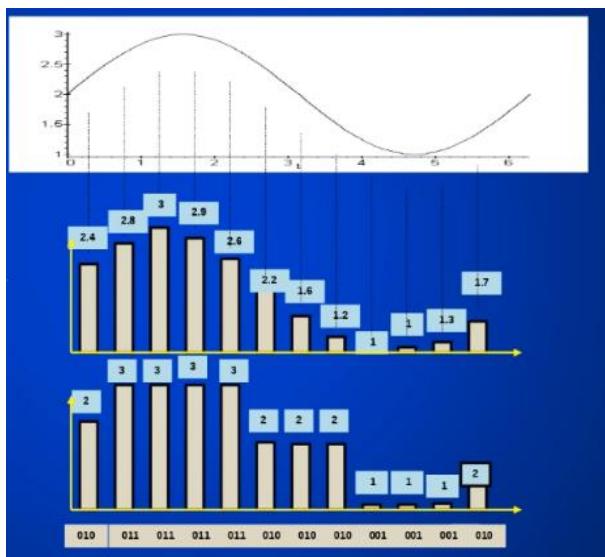
- ❖ **Códigos de bloques:** el codificador sustituye cada m bits por una palabra de n bits tal que n es mayor que m . Redundancia = $n-m$. Sirve para añadir sincronización entre emisor y receptor, para detectar errores, etc.



Datos analógicos/Señales digitales: Modulación por impulsos codificados

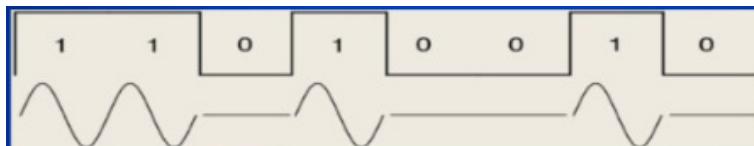
Tres etapas:

- ❖ Se muestrea la señal analógica: según el Teorema de Muestreo, la frecuencia de muestreo debe ser mayor o igual que el doble del ancho de banda. Se le asigna a cada número real tomado como muestra el valor entero más cercano correspondiente al nivel de cuantificación. Se produce por tanto un error de cuantificación.
- ❖ Se cuantifica la señal muestreada
- ❖ Los valores muestreados son codificados como flujo de bits

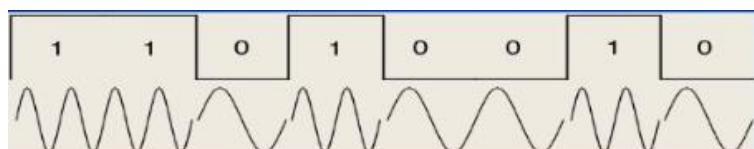


Dato digital/Señal analógica: el modulador (modem) genera una señal portadora acorde al medio de transmisión modificando amplitud, frecuencia o fase que se demodula en el destino.

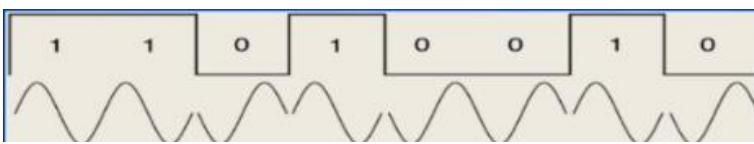
- ❖ **ASK (Amplitude Shift Keying):** los valores binarios se representan mediante dos amplitudes diferentes.



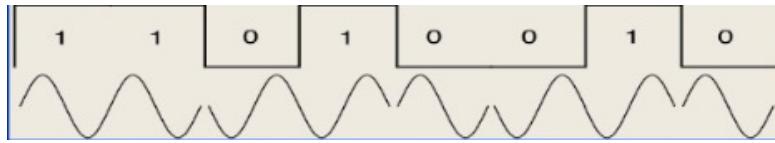
- ❖ **FSK (Frequency Shift Keying):** los valores binarios se representan mediante dos frecuencias diferentes.



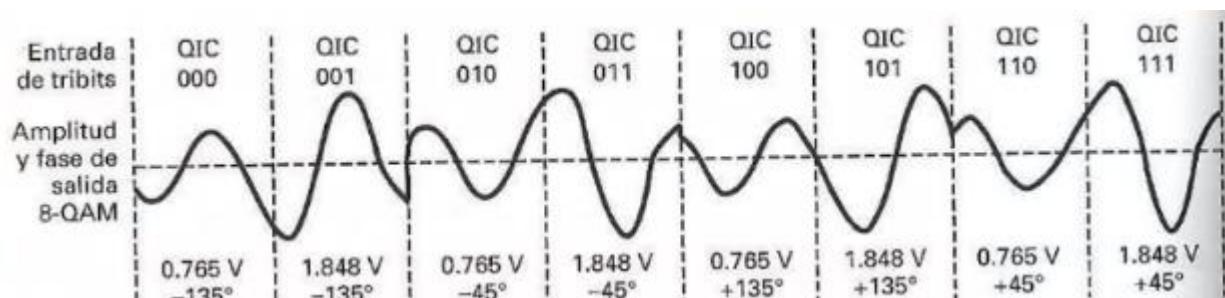
- ❖ **PSK (Phase Shift Keying):** los valores binarios se representan desplazando de fase la señal.



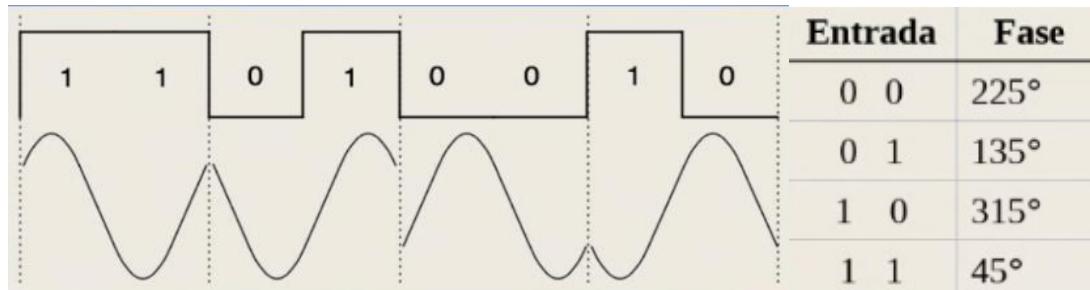
- ❖ **DPSK (Differential Phase Shift Keying):** los valores binarios representan desplazando de fase la señal según el estado anterior



- ❖ **QAM (Quadrature Amplitude Modulation)**: el modem genera dos portadoras desfasadas 90º y se modulan con ASK. Cada onda lleva una parte de los bits.



- ❖ **QPSK (Quadrature Phase Shift Keying)**: el valor se transmite rompiendo la fase

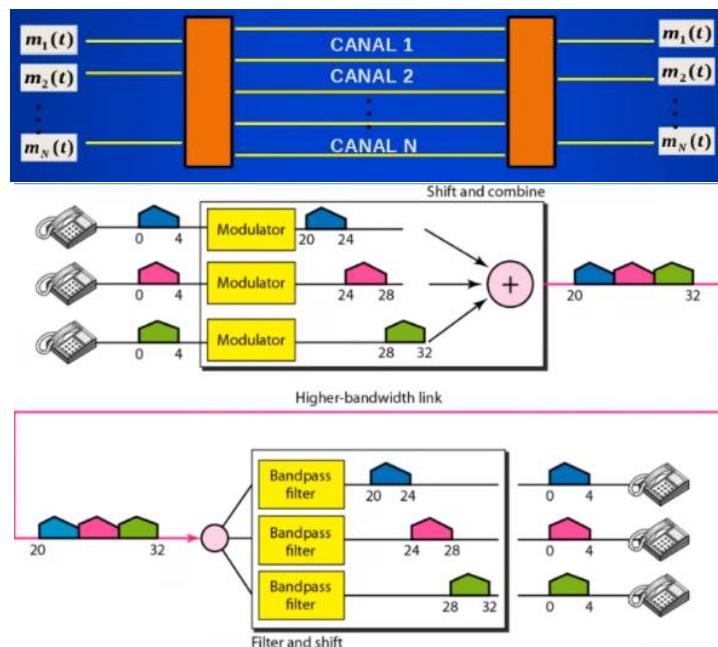


1.4 DISTRIBUCIÓN DE ANCHO DE BANDA

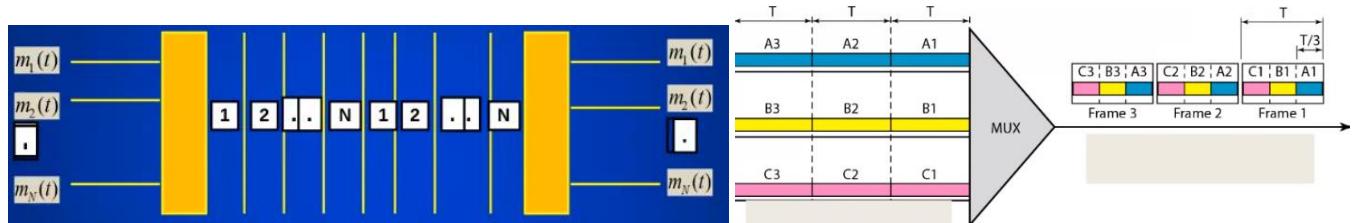
La limitación del ancho de banda depende de las características físicas del enlace. Para optimizar el uso de los enlaces se permite a varios usuarios usarlos a la vez. Cuando se usan medios guiados se busca la eficiencia en la transmisión, pero cuando se usan no guiados se busca la seguridad.

Multiplexación: permite combinar las señales de varias fuentes para conseguir un uso eficiente del ancho de banda. Permite transmitir de forma simultánea múltiples señales a través de un único enlace de datos.

- ❖ **División en frecuencia (MDF):** para señales analógicas. Es necesario que el ancho de banda del medio de transmisión sea mayor o igual que los anchos de banda de las señales a transmitir. El multiplexor modula la frecuencia de las distintas señales y las envía. A cada intervalo de frecuencias por el que se transmiten las distintas señales se le llama canal. Entre cada dos canales hay un intervalo por el que no se transmite nada, la banda de guardia.



- ❖ **División en el tiempo (MDT):** para señales digitales. El multiplexor asigna un intervalo de tiempo a cada línea conectada. A ese intervalo de tiempo se le llama canal. Al tiempo que transcurre entre dos canales de la misma línea se le llama trama. El multiplexor envía todas las señales a la vez de forma intercalada. En cada canal hay una muestra de la señal correspondiente. La siguiente muestra de una señal se manda tras acabar con la trama. Las señales comparten todo el ancho de banda.

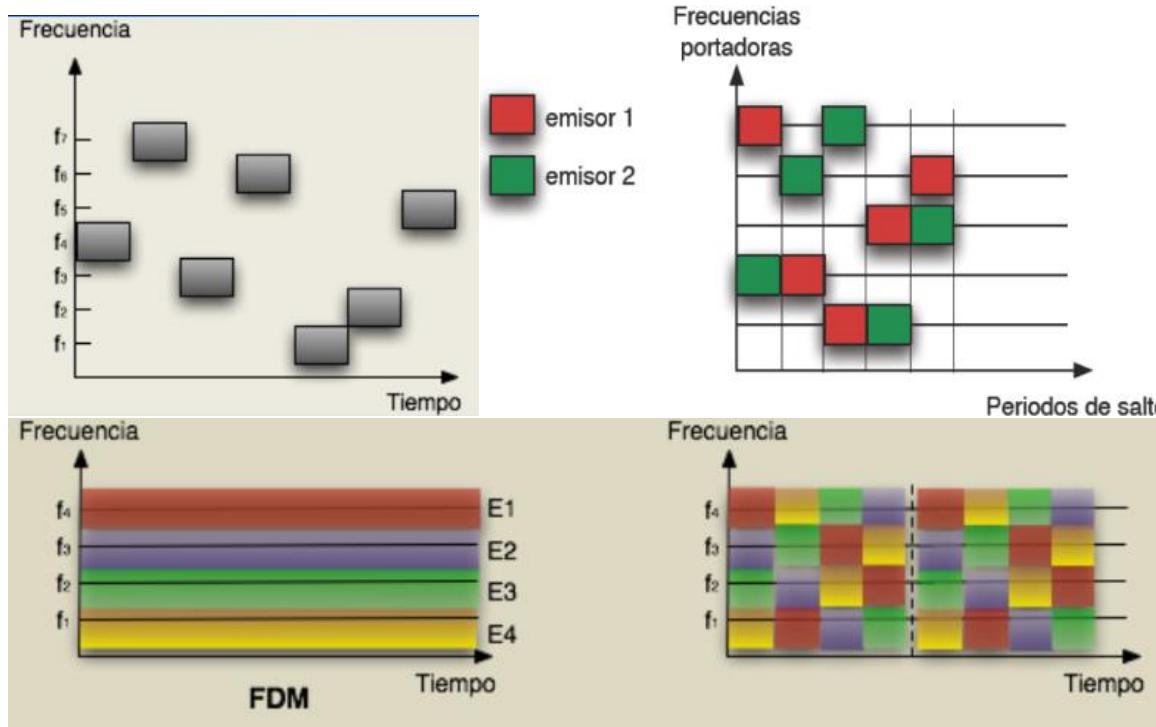


- ❖ **División en longitud de onda (WDM):** para datos analógicos o digitales cuando el enlace es fibra óptica. Transmite varios láseres con distintas frecuencias/longitudes de onda en la misma fibra óptica. Es como la división en frecuencia, pero en fibra óptica. La fibra óptica transmite en 3 ventanas de frecuencias (850, 1320, 1550nm), intervalos en los que la atenuación es constante.

- **Dense WDM (DWDM):** una versión que permite transmitir más canales.

Espectro expandido: las transmisiones inalámbricas necesitan de técnicas que garanticen sus seguridad e integridad. Se codifica la señal de modo que se incrementa de manera significativa el ancho de banda de la señal a transmitir con objeto de dificultar la interferencia e intercepción.

- ❖ **Salto de frecuencias:** para señales analógicas. Utiliza M frecuencias portadoras pseudoaleatorias saltando de frecuencia en frecuencia en intervalos fijos de tiempo. Las diferentes portadoras son moduladas por la señal origen. El receptor captará el mensaje saltando de frecuencia en frecuencia sincronizado con el emisor. Los receptores no autorizados captarán una señal ininteligible.



- ❖ **Secuencia directa DSSS (Direct Sequence Spread Spectrum):** para señales digitales. Cada bit de la señal original se representa utilizando varios elementos (minibits o chips) en la señal a transmitir mediante una secuencia pseudoaleatoria. El receptor usa una secuencia de código (código de expansión) que replica la del emisor. El código de expansión sirve para minimizar el efecto de las interferencias entre equipos de diferentes redes.

- **División de código CDMA (Code Division Multiple Access):** se tiene un código de expansión formado por una serie de 1 y -1. Cuando se transmite un 1 se envía el código de expansión tal cual, y cuando es un 0 el código de expansión cambiado de signo. El receptor realiza el producto escalar del código de expansión y lo recibido (multiplicar bit a bit los elementos de ambos vectores con el mismo índice y sumar los resultados). Si se obtiene un resultado positivo es 1 y si sale negativo es 0.

- Ej.: Código: 1,-1,-1,1,-1,1 | Datos [1 0] | Transmisión (1,-1,-1,1,-1,1), (-1,1,1,-1,1,-1)

$$(1,-1,-1,1,-1,1) * (1,-1,-1,1,-1,1) = 1+1+1+1+1 = 6 \rightarrow 1$$

$$(-1,1,1,-1,1,-1) * (1,-1,1,1,-1,1) = -1-1-1-1-1 = -6 \rightarrow 0$$

Si el mensaje lo transmiten varias estaciones con distintos códigos de expansión se suman los vectores transmitidos por cada estación y se calculan los productos escalares del vector resultante por los códigos de expansión de cada estación.

- Ej.: Tres estaciones transmiten: (-1,-1,-1,1,1,-1,1,1), (1,1,-1,1,-1,-1,1,1), (-1,1,1,-1,1,1,1,-1,-1)

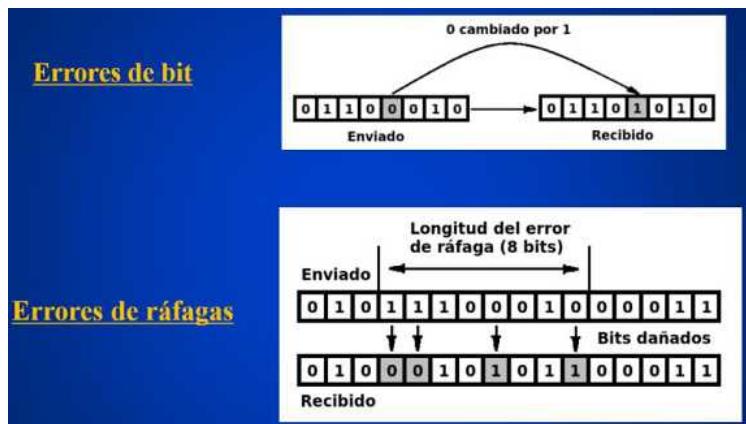
El receptor recibe la suma de los 3 vectores: (-1,1,-3,3,1,-1,-1,1)

El receptor multiplica el vector suma por los códigos de expansión de cada estación, (-1,-1,-1,1,1,-1,1,1), (-1,-1,1,-1,1,1,1,-1), (-1,1,1,-1,1,1,1,-1), y obtiene 8, -8 y 8. Por tanto descifra [1 0 1].

1.5 TÉCNICAS DE COMUNICACIÓN DE DATOS

Los sistemas fiables deben tener mecanismos para garantizar la integridad de la transmisión detectando y corrigiendo errores que se hayan generado entre la emisión y la recepción. El emisor emite una carga extra en la transmisión llamada redundancia. Esta redundancia consiste en emitir bits adicionales llamados bits de redundancia que sirven para detectar en el destino si ha habido errores. Los errores pueden ser de dos tipos:

- ❖ **Errores de bit:** afectan un único bit.
- ❖ **Errores de ráfagas:** afectan a varios bits de la secuencia.



Distancia de Hamming $d(v_1, v_2)$: es el número de bits en el que difieren dos secuencias binarias v_1 y v_2 . Para cada código válido se calcula su distancia de Hamming con los demás y de entre ellas se obtiene la mínima distancia de Hamming. Esta distancia permite garantizar que una transmisión es errónea.

- ❖ Se pueden detectar hasta t errores siendo $t = d_{min} - 1$.
- ❖ Se pueden corregir hasta t errores siempre que $d_{min} \geq 2t - 1$

Mecanismos de control de errores:

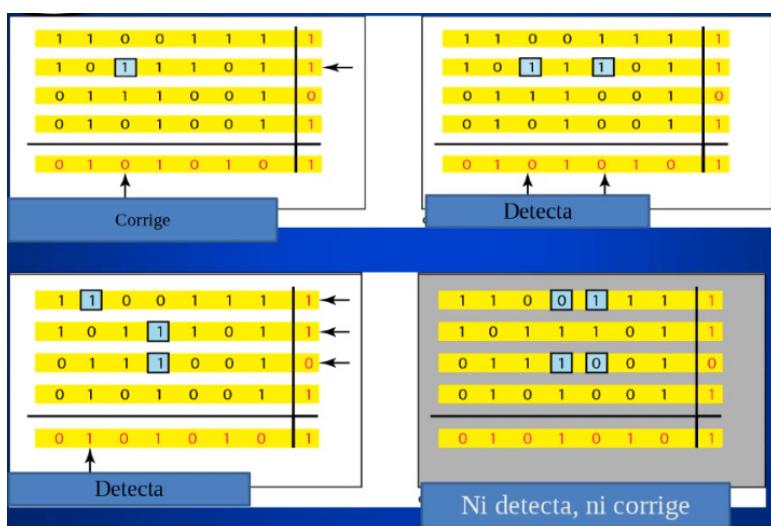
- ❖ **Automatic Repeat Request (ARQ):** solo detectan errores de transmisión (bits cambiados). Requieren menos información adicional o redundancia. Utiliza los protocolos TCP. La detección de errores consiste en la adición de redundancia a los mensajes y la recuperación se hace mediante retransmisión. Hay dos técnicas:
 - **Comprobación de paridad:** añade un bit de paridad al final del bloque de datos. Solo detecta números impares de errores.
 - **Paridad impar:** el valor del bit añadido se determina de modo que el número total de 1s sea impar.
 - **Paridad par:** el valor del bit añadido se determina de modo que el número total de 1s sea par
 - **Comprobación de redundancia cíclica (CRC):** los bits de redundancia se generan en función del polinomio generador $G(x)$ que se haya elegido para codificar la información. Dado un mensaje de m bits el emisor genera una secuencia de r bits. La trama resultante de $m+r$ bits será divisible por algún número determinado. El receptor divide la trama por ese número y si no hay resto no detecta errores (puede haberlos, pero no los detecta).

<ul style="list-style-type: none"> • Sea: <ul style="list-style-type: none"> – $M(x)$: mensaje original (m bits) – $G(x)$: polinomio generador ($r+1$ bits) – $T(x)$: mensaje a transmitir ($m+r$ bits) • En emisión: • En recepción: 	$T(x) = M(x) \cdot x^r + R(x) \quad \text{siendo} \quad R(x) = \text{mod}\left(\frac{M(x) \cdot x^r}{G(x)}\right)$ $R'(x) = \text{mod}\left(\frac{T(x)}{G(x)}\right)$ <p style="text-align: center;">Si $R'(x) = 0$, no hay errores Si $R'(x) \neq 0$, hay errores</p>	$\begin{array}{r} M(X)=X^6 + X^3 + 1 \\ G(X)=X^3 + X + 1 \\ \hline 1001001000 \\ 1011 \\ \hline 001000 \\ 1011 \\ \hline 001110 \\ 1011 \\ \hline 01010 \\ 1011 \\ \hline 00010 \\ 00010 \end{array}$ $= R(X)$
---	--	--



Detectan errores de un único bit, errores dobles si $G(x)$ tiene al menos tres 1s, número impar de errores siempre que $G(x)$ tenga el factor $(x+1)$, ráfagas de errores de longitud menor que la longitud de $G(x)$ y la mayoría de las ráfagas de longitud mayor.

- ❖ **Forward Error Correction (FEC):** detectan y corrigen errores de transmisión (bits cambiados). Requiere mucha información adicional o redundancia. Utiliza redes móviles. La protección de errores consiste en la adición de redundancia para detectar un corregir errores. Hay dos técnicas
- **Códigos de doble paridad:** el codificador genera una matriz y se calcula doble paridad por fila y columna.



- **Códigos de Hamming:** siendo m el número de bits del mensaje y r los bits de redundancia:

$$m + r + 1 \leq 2^r$$

Los bits cuya posición es potencia de dos se utilizan como bits de paridad (incluido 2^0) y el resto como bits de datos. El valor de los bits de redundancia se obtiene comprobando la paridad (par o impar) de un conjunto de bits determinado por el siguiente algoritmo:

El bit n salta $n-1$, comprueba n , salta n , comprueban, salta n , etc.

Ej.: r1 r2 0 r3 1 1 0 r4 1 0 1

1 comprueba la paridad de 1,3,5,7,9,11

2 comprueba la paridad de 2,3,6,7,10,11

4 comprueba la paridad de 4,5,6,7

8 comprueba la paridad de 8,9,10,11

2. ARQUITECTURA TCP/IP

2.1 REDES Y ARQUITECTURAS

Red: medio físico de comunicación y compartición de recursos de información y computación entre equipos.

Equipo: cualquier dispositivo conectado a una red, direccionable (con una dirección en dicha red) capaz de hablar un mismo idioma con otros equipos conectados a la misma red mediante mensajes pertenecientes a un mismo conjunto de protocolos de comunicación.

Dos tipos de redes:

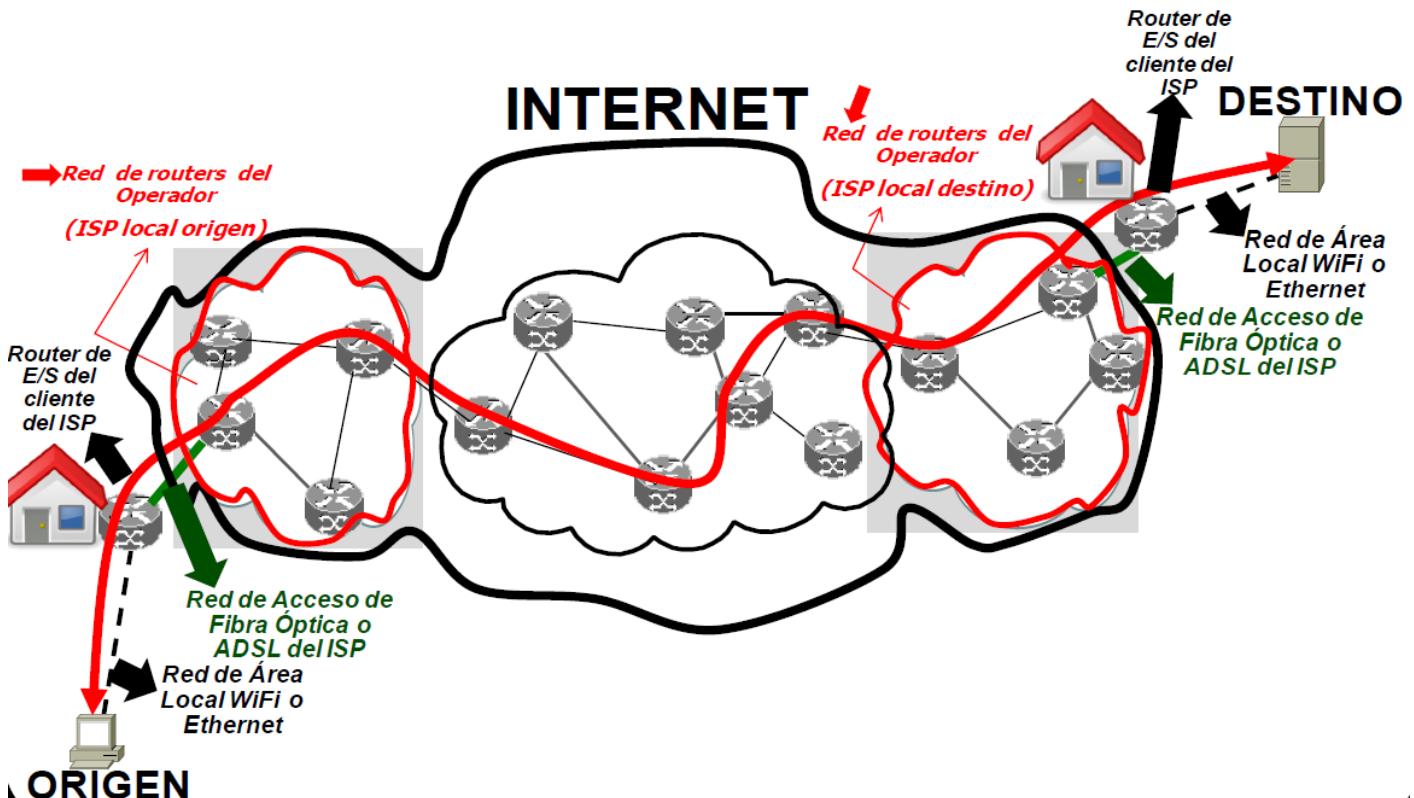
- ❖ **Redes físicas:** equipos conectados por cable o inalámbricamente
 - **Ethernet (Internet):** conectan directamente equipos de usuario, acceden a Internet y conectas routers en Internet.
 - **WiFi (Accesos a Internet):** conectan directamente equipos de usuario y acceder a Internet
- ❖ **Redes de computadoras:** son redes abstractas que engloban un número indeterminado de redes de comunicaciones (Ethernet) conectadas por equipos intermedios (routers).

Internet: red abstracta lógica o virtual que engloba equipos intermedios o routers (gateways) conectados a través de redes de comunicaciones (Ethernet) con protocolo TCP/IP.

Router: equipo intermedio que encamina unidades de datos en función de la dirección del equipo final destinatario.

Equipos finales: deben estar conectados a un router, tener una dirección con un formato común de direccionamiento y tener instalados un conjunto común de protocolos de comunicaciones.

Proveedor de acceso a internet (ISP): operador global de telecomunicaciones que ofrece acceso a internet a sus clientes mediante una red de routers distribuida por el país. Las conexiones ethernet entre las correspondientes redes de routers de los ISPs permiten la formación de la red virtual Internet.



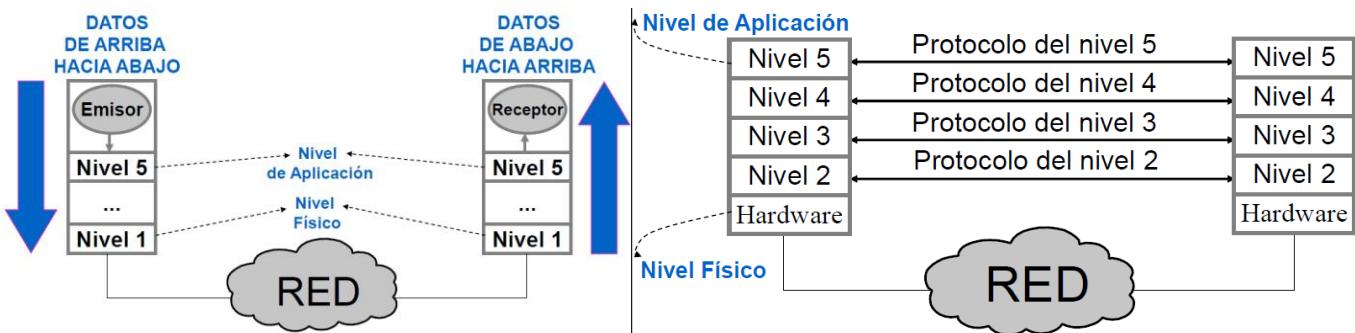
2.2 ARQUITECTURAS ESTRUCTURADAS DE COMUNICACIONES

Una arquitectura estructurada de comunicaciones es un conjunto de protocolos de comunicaciones que se ejecutan de forma independiente en diferentes niveles, exceptuando el nivel más elemental o nivel físico o de hardware. La estructuración en niveles reduce la complejidad del software de comunicaciones y favorece la labor de diseño mediante una estructura más comprensible en diferentes niveles de comunicaciones mutuamente independientes. Diferentes equipos se comunican a través de diferentes niveles. También facilita el cambio tecnológico ya que los cambios realizados en un nivel no afectan al resto de niveles. La arquitectura TCP/IP se organiza de la siguiente manera:

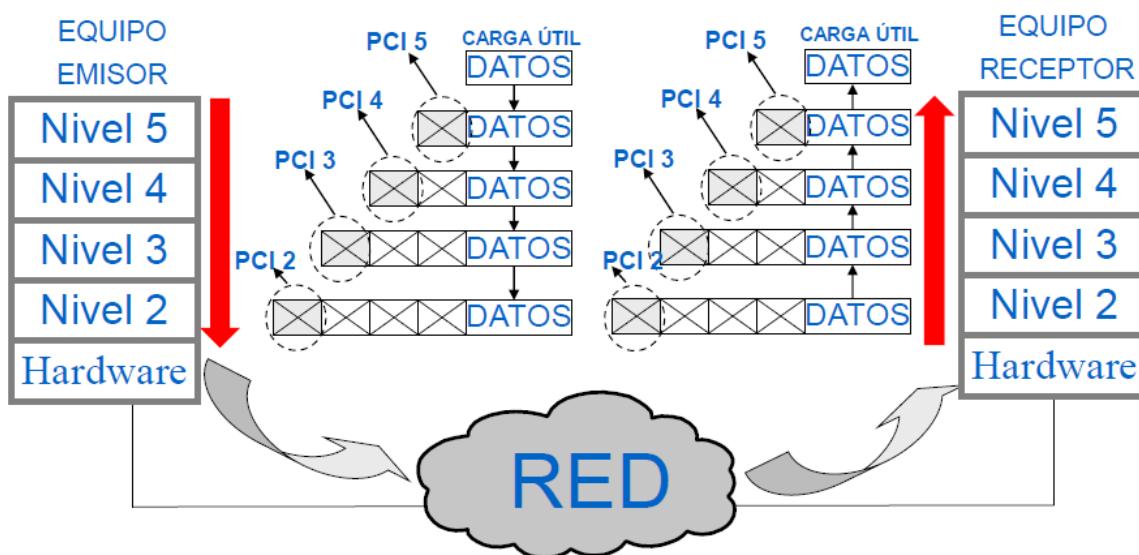
Entidades pares: dos procesos que ejecutan el mismo protocolo de comunicaciones y se comunican por el mismo nivel.

Protocolo de comunicaciones: conjunto de reglas que definen el formato y orden de las unidades de datos intercambiadas entre entidades pares que se ejecutan en equipos diferentes, así como las funciones o acciones que tienen que llevar a cabo dichas procesos iguales o entidades pares para proporcionar un determinado servicio.

Comunicación entre distintos niveles: se envían los datos de arriba hacia abajo en el equipo emisor y de abajo hacia arriba en el receptor. La comunicación efectiva es entre niveles equivalentes. Los niveles inferiores solo procesan la información para llevarla al nivel físico y poder transmitir. Entre ambos extremos y para cada nivel (salvo el nivel físico) existen dos entidades pares o iguales que ejecutan un protocolo de comunicaciones que define el formato de los mensajes, su orden y acciones o funciones.

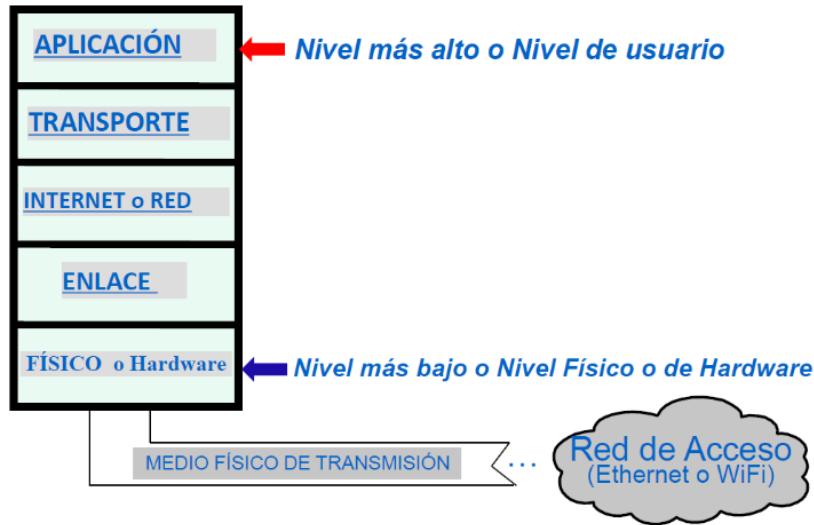


Unidad de datos de protocolo (PDU): unidad completa de información intercambiada por entidades pares. Contiene una cabecera (PCI-Protocol Control Information) con información de control y los datos (SDU-Service Data Unit). Una PDU de un nivel determinado contiene las PCIs y SDUs de los niveles superiores. El equipo emisor añade cabeceras de información de control en cada nivel salvo en el físico. El equipo receptor, en cada nivel salvo en el físico, realiza las funciones indicadas según la cabecera recibida, elimina la cabecera y pasa el resto al nivel inmediatamente superior.



2.3 ARQUITECTURA TCP/IP

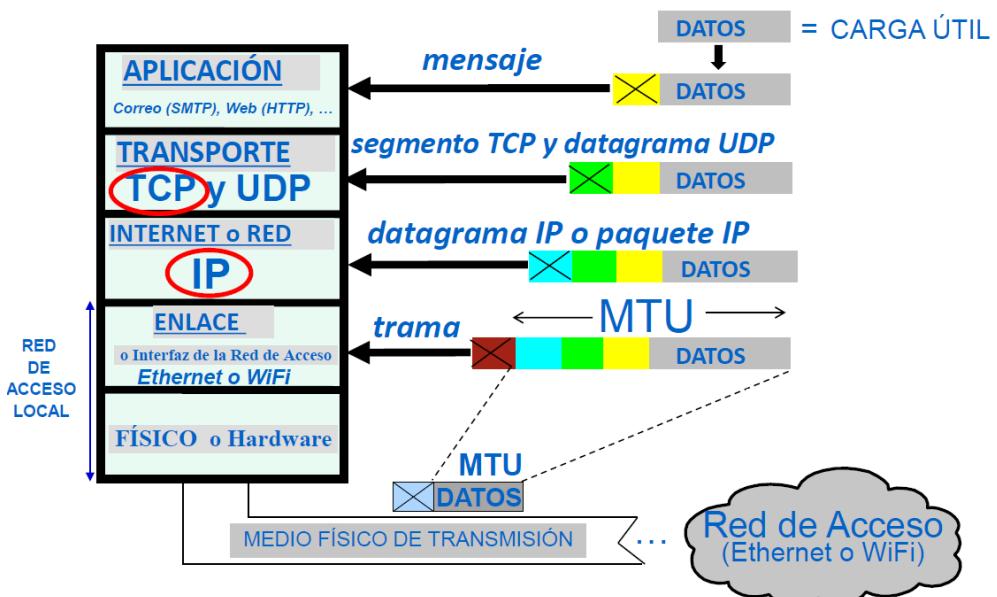
Es una arquitectura estructurada en cinco niveles:



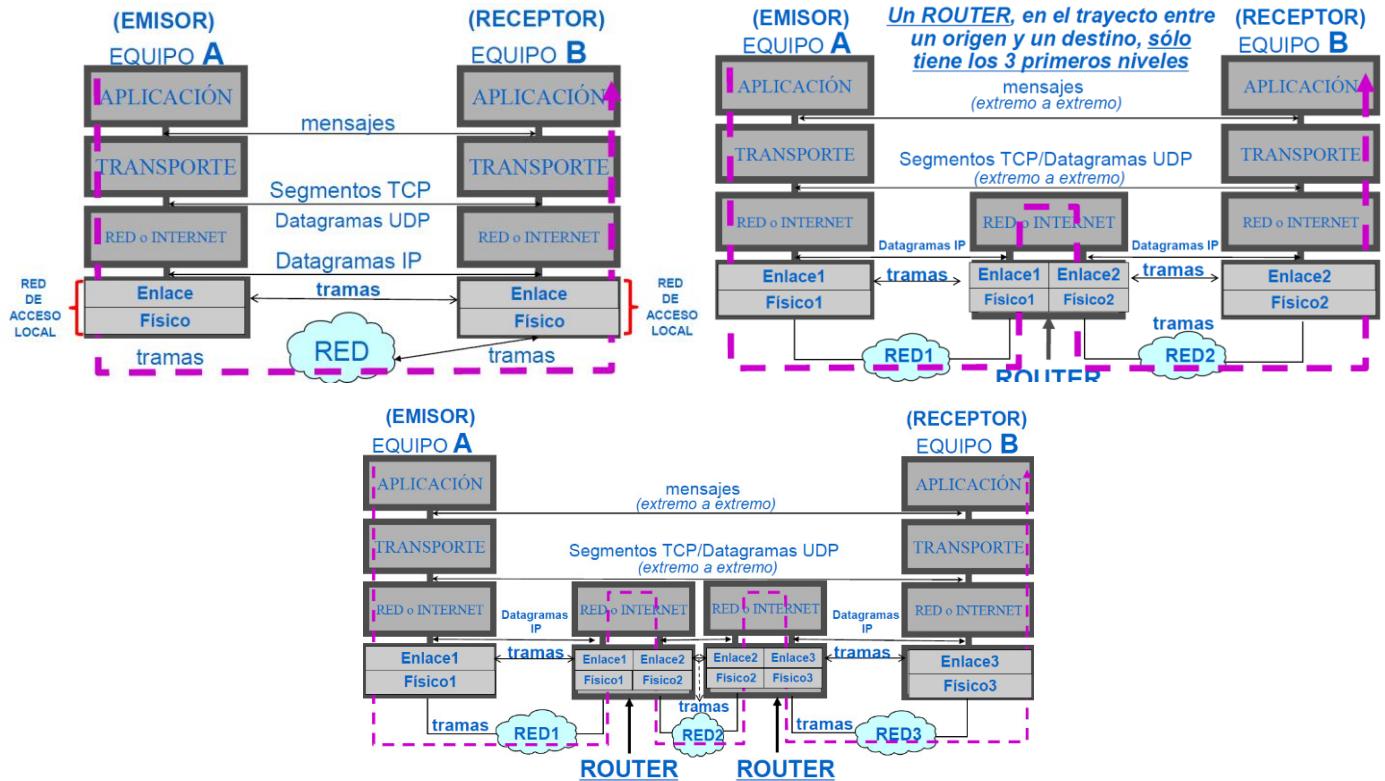
Protocolos y formato de las PDUs: los datos que se quieren transmitir reciben el nombre de carga útil. A esos datos los protocolos de cada nivel les añaden cabeceras:

- ❖ **Aplicación:** se le añade una cabecera de control en función del tipo de datos. Si es un correo se añade según el protocolo SMTP, si es una web el HTTP, etc. A esa PDU con la cabecera se la conoce como mensaje.
- ❖ **Transporte:** se añade otra cabecera TCP o UDP según el tipo de transporte y la PDU pasa a conocerse como segmento TCP o datagrama UDP. El protocolo TCP realiza un transporte fiable segmentando los mensajes, si procede, en función de la máxima unidad de transporte (MTU). A cada fragmento se le añade una cabecera. El protocolo UDP realiza un transporte no fiable pero más rápido.
- ❖ **Red:** se añade una IP, que es el protocolo que sirve para encaminar en Internet hacia el equipo final destino, llamándose esta nueva PDU datagrama o paquete IP.
- ❖ **Enlace:** se añade otra nueva cabecera Ethernet o WiFi que encamina la información por la red de acceso hacia una dirección MAC, también conocida como dirección física. La PDU recibe el nombre de trama.

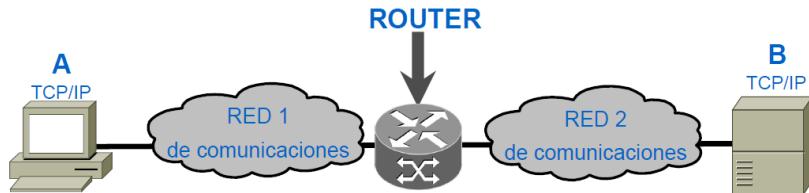
En Ethernet no se pueden enviar más de 1500 bytes. Si se quiere enviar un archivo más pesado hace a trozos. A este límite se le conoce como MTU. La MTU la ocupa el paquete IP, la cabecera añadida por el protocolo de enlace no cuenta.



Los routers solo tienen los tres primeros niveles. Si hay routers entre el emisor y el receptor a nivel de transporte y aplicación se comunican entre si sin importar lo que haya en medio, pero a nivel IP el emisor no se comunica con el receptor, sino con el router más cercano que pueda direccionar a B. El protocolo de enlace puede cambiar en los routers, que, por ejemplo, pueden recibir la información por WiFi y enviarla por Ethernet. Las siguientes imágenes muestran ejemplos de equipos conectados dentro de la misma red y equipos conectados a través de Internet por uno y dos routers.



Todo equipo TCP/IP tiene tantas direcciones del nivel de red y del nivel de enlace como redes de comunicaciones a las cuales esté conectado. En un caso como el de la siguiente imagen A tiene una dirección del nivel de red IP y otra de nivel de enlace para RED1. B igual, pero para RED2. Sin embargo, el router tiene dos direcciones IP y dos direcciones de enlace, unas para RED1 y otras para RED2.

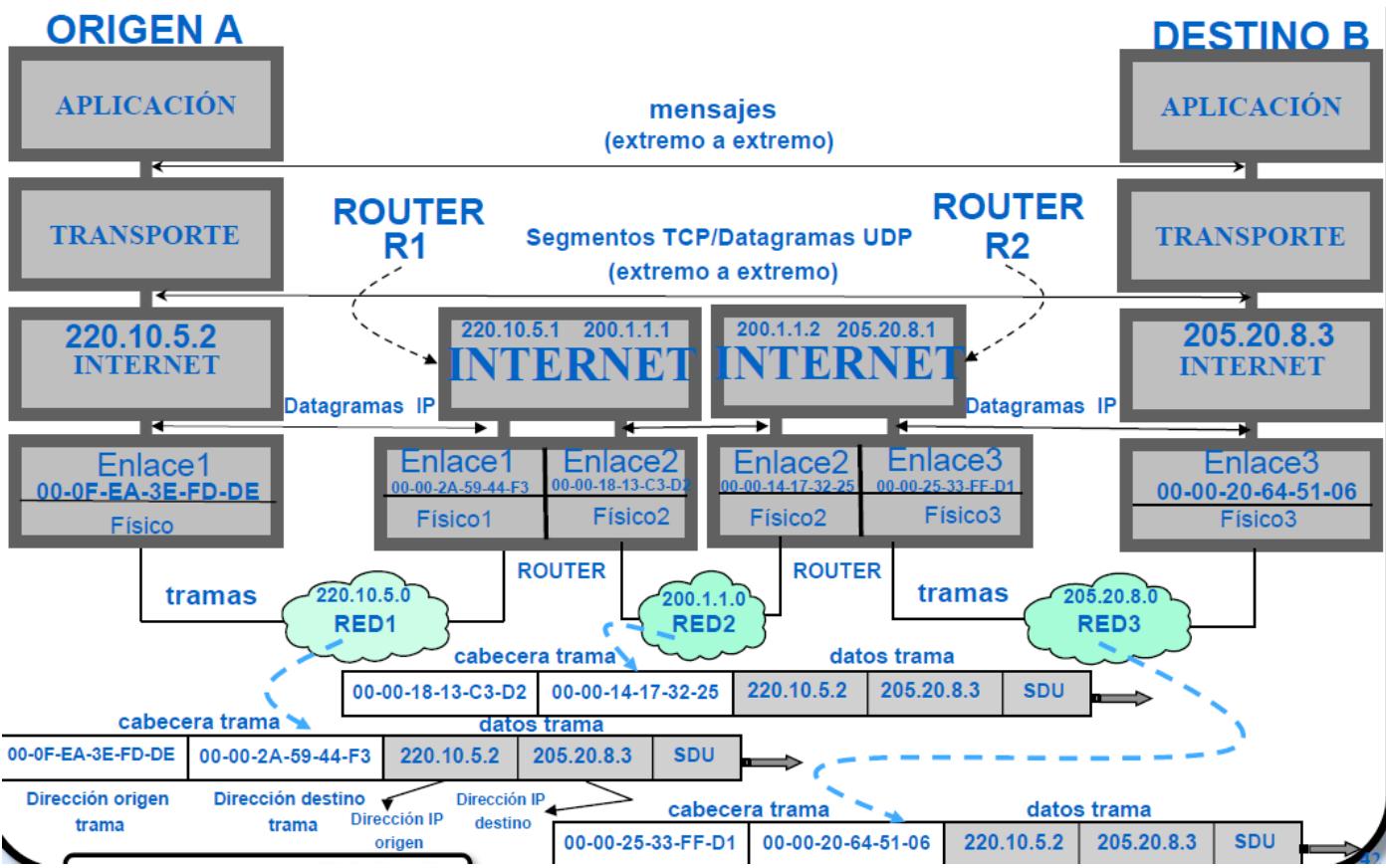


Toda entidad IP tiene una tabla de encaminamiento IP que le permite saber hacia qué router enviar la información para llegar a su destino. Una entidad de nivel de enlace captura cualquier trama con su dirección MAC.

Dirección MAC: conocida también como dirección física, está asignada a la tarjeta de red. Nunca cambia independientemente de la red a la que se conecte. Formato de 6 bytes, en el que cada byte es un número hexadecimal de dos dígitos. Los tres primeros los asigna el IEEE y los tres últimos el fabricante. Por ejemplo: 00:0F:EA:3E:FD:DE.

Dirección IP: asignada a cada equipo por el administrador de la red a la que esté conectado. Es la dirección del equipo en donde se ejecuta un proceso TCP/IP. Si el equipo se conecta a otra red de comunicaciones cambia su dirección IP. Formato de 4 bytes donde cada byte es un entero entre 0 y 255. Depende del prefijo de la dirección IP de la red. Por ejemplo, si el prefijo de red es 220.10.5.0, una dirección válida para un equipo de la red sería 220.10.5.1.

Si un envío de información tiene que pasar por un router las direcciones MAC de la PDU van cambiando en función del origen y el destino inmediatos, pero las direcciones IP son siempre la original y la final.



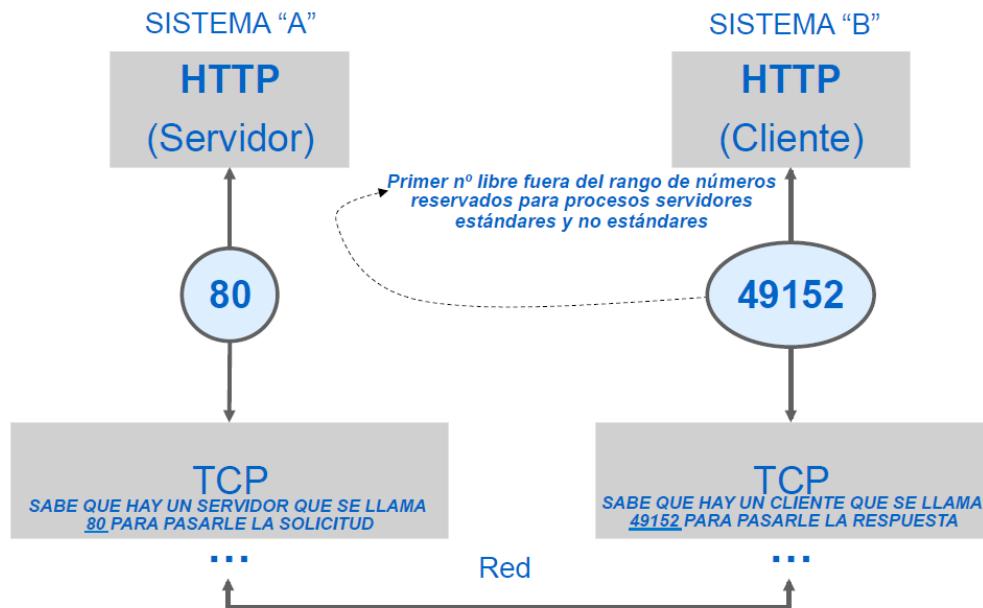
Niveles superiores e inferiores: llamamos superiores a los niveles de aplicación y transporte e inferiores a los de red y enlace. La diferencia es que la comunicación entre los superiores es de extremo a extremo. Esto significa que mientras que en los niveles inferiores la comunicación se hace a través routers intermedios que hacen uso de las direcciones de esos niveles, en los superiores la información de origen solo se procesa en el destino.

Protocolos de niveles inferiores:

- ❖ **Red:**
 - **IP:** para el encaminado de paquetes IP en internet.
 - **ICMP:** para el envío de mensajes de control en internet, generalmente cuando surge un problema con IP.
- ❖ **Enlace:**
 - **Ethernet y WiFi.**
 - **PPP:** en líneas punto a punto (ADSL telefónicas y fibra óptica) en donde se conectan solo dos equipos.
 - **ARP:** Permite obtener automáticamente la dirección del nivel de enlace o dirección MAC (media access control) asociada a la dirección IP de un equipo vecino en una red del tipo Ethernet o WiFi.

Nivel de aplicación: aquí funcionan la mayoría de las aplicaciones en Internet (salvo utilidades o herramientas TCP/IP como ipconfig/ifconfig/netstat, ping, etc.). Funcionan según el modelo cliente-servidor. El proceso cliente envía al proceso servidor una solicitud específica de servicio y el proceso servidor proporciona un servicio como respuesta. Las entidades se montan sobre TCP si se desea un transporte fiable o sobre UDP si se desea un transporte rápido.

Número de puerto: los procesos cliente y servidor están identificados por un número de puerto. Es un entero positivo de 16 bits manejado por TCP y UDP. Algunos están reservados para procesos servidores estándar en Internet, como por ejemplo el 25, que es utilizado para identificar al proceso servidor de correo electrónico SMTP, o el 80 para HTTP, en cualquier máquina por Internet. Del 0 al 1023 son para procesos servidores estándar en Internet, del 1024 al 49151 son para procesos servidores no estándares en Internet y del 49152 al 65535 son para procesos clientes.



Socket: identificador local del extremo de una comunicación en Internet para un proceso de aplicación cliente o servidor montado en RCP o UDP. Está definido por el protocolo de transporte, por la dirección IP del equipo y por el número de puerto. Por ejemplo, un socket sería TCP, 138.10.1.16 : 80.

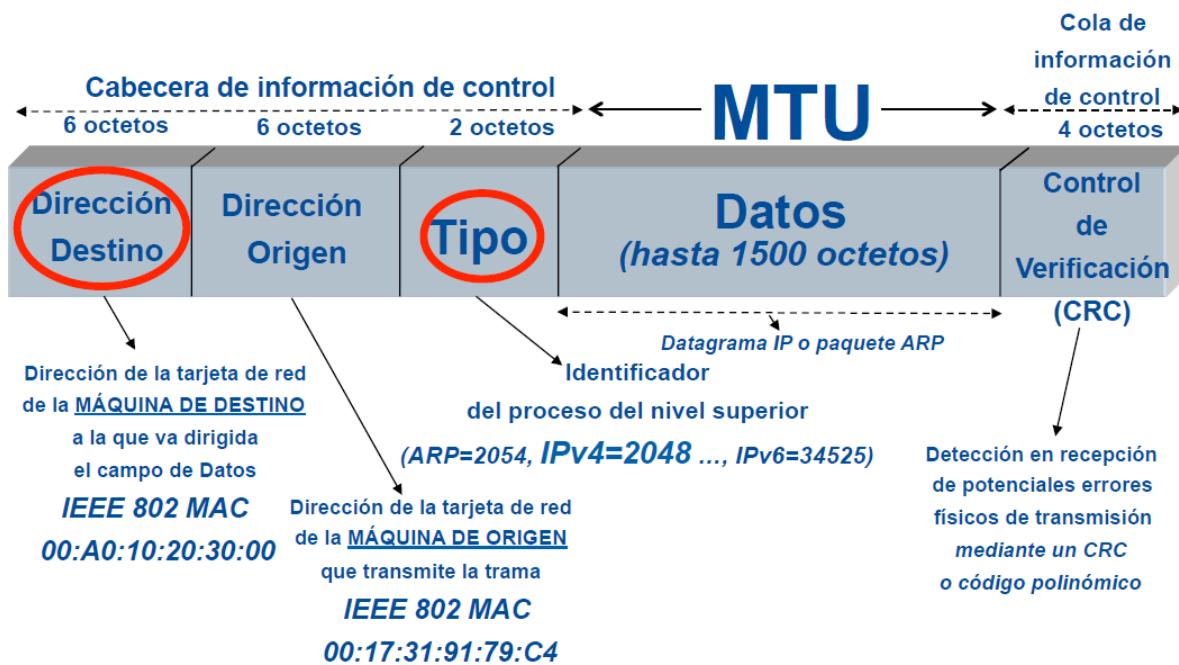
2.4 NIVEL DE ENLACE

El conjunto de los niveles de enlace y físico se conoce como red de acceso local. Cada tarjeta red tiene un identificador único (dirección MAC) puesto por el vendedor. La tarjeta de red contiene el protocolo Ethernet o WiFi que se usa en el nivel de enlace.



Protocolos de nivel de enlace: dos equipos vecinos deben comunicarse usando el mismo protocolo.

- ❖ **Ethernet:** servicio no fiable. Las probabilidades de error en la transmisión son ínfimas. No hay control de fallos físicos (ni recepción ni recuperación) en las tramas recibidas. Solo detecta fallos físicos de transmisión o bits cambiados, pero no se corrigen o se recuperan, sino que dicha trama se desecha. No hay control de fallos lógicos (tramas perdidas, desordenadas y duplicadas). No hay control de flujo, no evita que una entidad Ethernet transmita más rápido de lo que otra es capaz de almacenar y procesar. Formato de trama Ethernet:



- ❖ **WiFi:** servicio fiable. Hay control (detección y recuperación) de fallos físicos (bits cambiados) en las tramas recibidas. Incluye control de fallos lógicos (detección y recuperación de tramas perdidas, desordenadas y duplicadas). Hay control de flujo, evita que una entidad WiFi transmita más rápido de lo que otra puede almacenar y procesar.
- ❖ **PPP:** protocolo en líneas o redes de acceso telefónicas vía ADSL o de fibra óptica vía luz modulada (señales ópticas). Por omisión ofrece un servicio no fiable porque la probabilidad de interferencia es despreciable. Se puede configurar un modo fiable a costa de velocidad.

2.5 NIVEL DE RED

Protocolo IP: Encaminamiento no fiable pero rápido por Internet en función de la dirección IP del destinatario. El encaminamiento es siempre entre dos equipos vecinos conectados a la misma red de acceso en el trayecto entre origen y destino.

- ❖ **IPv4:** protocolo en uso actualmente pero que ha alcanzado el final de su vida operativa.
- ❖ **IPv6:** protocolo de encaminamiento para uso futuro. Las principales diferencias con respecto a IPv4 son que las direcciones pasan de 4 a 16 bytes, mayor flexibilidad y rapidez en el encaminamiento gracias a una cabecera de información de control más simple con la mitad de campos y mayor seguridad.

Doble pila IPv4/IPv6: instalada en cualquier sistema operativo actual.

Tipos de transmisiones IPv4:

- ❖ **Unidifusión (Unicast):** todas las transmisiones en Internet son de este tipo. Transmisiones punto a punto entre dos equipos. Si queremos enviar un mismo paquete IP a n destinatarios habrá que realizar n envíos con n copias del mensaje.
- ❖ **Multidifusión (Multicast):** transmisión a un grupo de equipos que comparten una misma dirección multicast. Si se quiere enviar un paquete IP desde un equipo (servidor multicast) a varios destinatarios podemos realizar un único envío si tienen la misma dirección multicast. En el campo de dirección de destino del paquete IP va la dirección multicast.
- ❖ **Difusión (Broadcast):** transmisión a todos los equipos vecinos de una red de acceso ethernet o WiFi mediante un solo envío sin copias desde el origen. En el campo de dirección destino del paquete IP va la dirección IP 255.255.255.255.

Correspondencias IP-MAC: la dirección MAC en casos de difusión será FF-FF-FF-FF-FF-FF y casos de multidifusión empieza por el prefijo 01-00-5E

Dirección IPv4: engloba la dirección de red y la dirección de máquina. Tanto las redes como las máquinas tienen direcciones IP. Formada por 4 bytes separados por puntos. En función de la clase de transmisión existen 5 clases de direcciones IP. A, B y C para unidifusión y difusión, D para multidifusión y E experimental o reservada.

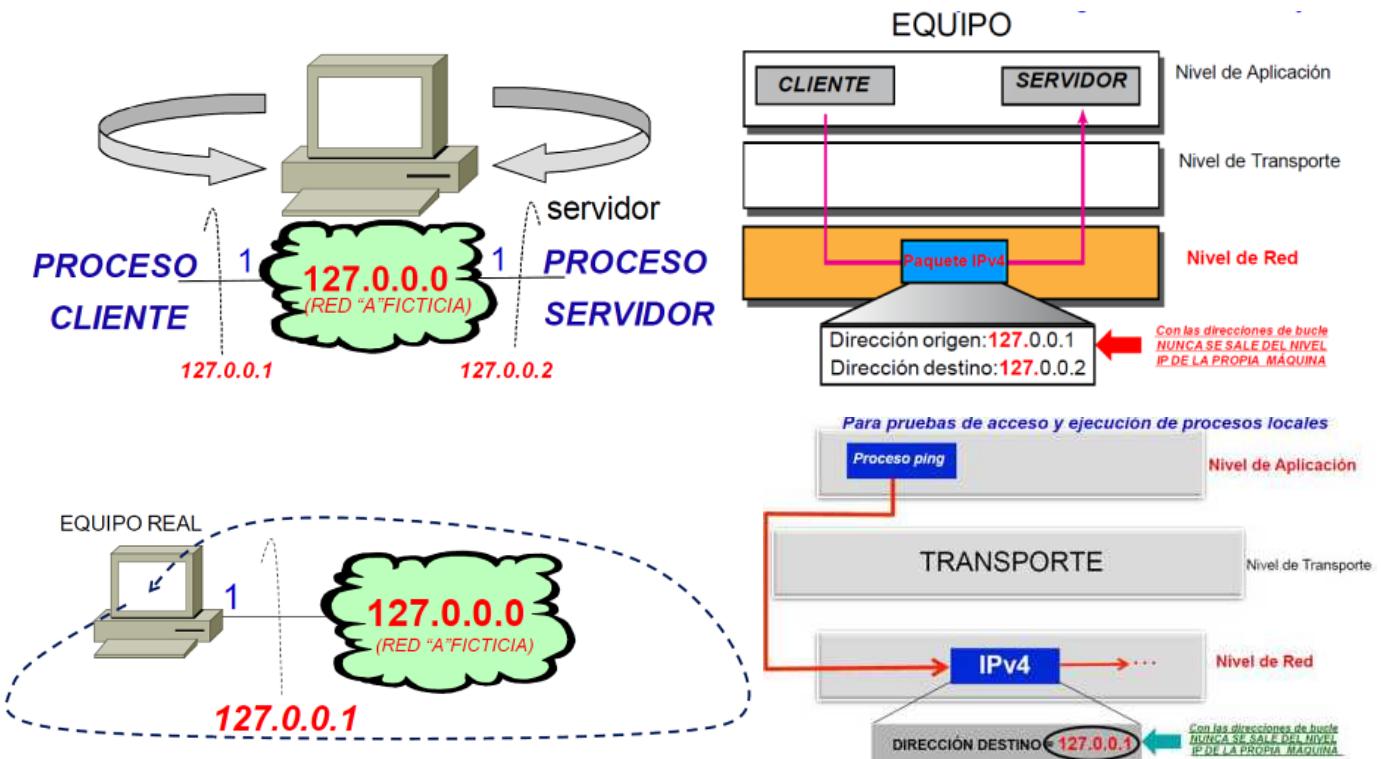
- ❖ **Clase A:** su primer byte en decimal va del 1 al 126 (0 y 127 reservados). El primer byte se usa para identificar redes y los tres restantes para equipos.
- ❖ **Clase B:** su primer byte en decimal va del 128 al 191. Los dos primeros bytes se utilizan para identificar redes y los dos últimos para identificar equipos.
- ❖ **Clase C:** su primer byte en decimal va del 192 al 223. Los tres primeros bytes se utilizan para identificar redes y el último para equipos.



- ❖ Clase D: su primer byte va del 224 al 239. El resto lo ocupa la dirección multicast del grupo.
- ❖ Clase E: su primer byte va del 240 al 255. No se usan salvo para investigación y experimentación.

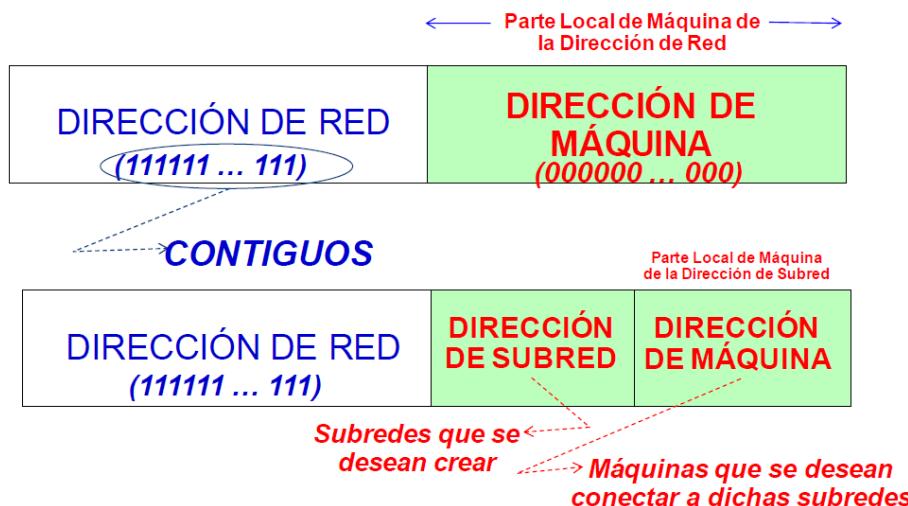
Direcciones reservadas:

- ❖ Direcciones reservadas de red clase A:
 - 0.0.0.0: ruta por omisión en una tabla IP o una solicitud de configuración TCP/IP vía cliente DHCP.
 - 127.0.0.0 es una dirección de red de bucle o red de loopback. Es una dirección IP ficticia de equipo perteneciente a una red también ficticia para desarrollar procesos clientes y servidores IP ficticios probando su interacción o para probar el acceso a la máquina y sus procesos locales.



- ❖ En el campo de dirección máquina todo 0s indica que es una dirección de red y todo 1s que es una difusión.
- ❖ 255.255.255.255: para difusión limitada a la red de la máquina origen.

Subredes: una subred es un subconjunto de una red de comunicaciones. Será de la misma clase que la red a la que pertenece. El administrador crea las subredes y asigna direcciones IP a dichas subredes a partir de la dirección IP pública de red asignada por el ISP a la red y del número de 0s de la máscara asociada a dicha dirección. La parte local de la dirección se divide en dos partes, una para la dirección de subred y otra para la dirección de máquina.



Máscaras: toda dirección IP tiene una máscara asociada. Hay 4 tipos de máscaras para los 4 tipos de direcciones IP: de red, de subred, de superred y de máquina.

- ❖ **De red:** la máscara es un número de 32 bits que contiene 1s en los bits que identifican la parte de red y 0s en los bits que identifican la parte local o de la dirección máquina. Para representar la máscara de una dirección IP se le añade /nº bits de la dirección de red.
- Ej.: 20.0.0.0/8 (Clase A), 136.15.0.0/16 (Clase B), 220.10.1.0/24 (Clase C) cuyas máscaras serían 255.0.0.0, 255.255.0.0 y 255.255.255.0 respectivamente.



- ❖ **De máquina:** la máscara es un número de 32 bits que contiene 1s en los bits que identifican la dirección máquina. Una máquina utiliza los 32 bits de una dirección IP, por tanto, los 32 estarán a 1.
- Ej.: 136.15.22.3/32 con máscara 255.255.255.255
- ❖ **De subred:** la máscara es un número de 32 bits que contiene 1s en los bits que identifican la parte de subred y que se añaden a los 1s que identifican la parte de red. Cuando se quiere crear un cierto número de subredes se coge de la parte local de la dirección de red el número de bits necesarios para representarlas y se añaden a la máscara. Los bits restantes serán las direcciones locales de los equipos de esas subredes.
- Ej.: De la red 220.20.8.0/24 se quieren hacer 6 subredes. La nueva máscara será /27, o lo que es lo mismo 255.255.255.224 = 11111111 11111111 11111111 11100000. Las direcciones de las subredes se sacan como se indica en la imagen:

$000 = \text{SE PUEDE USAR} = 0$ $001 = 2^5 = 32$ $010 = 2^6 = 64$ $011 = 2^6 + 2^5 = 96$ $100 = 2^7 = 128$ $101 = 2^7 + 2^5 = 160$ $110 = 2^7 + 2^6 = 192$ $111 = \text{SE PUEDE USAR} = 224$	$220.10.8.32$ $220.10.8.64$ $220.10.8.96$ $220.10.8.128$ $220.10.8.160$ $220.10.8.192$
---	---

La dirección del router de cada subred será la primera de cada subred (220.10.8.33 por ejemplo), el resto serán para máquinas (220.10.8.34-62 por ejemplo) excepto la última que será para broadcast en esa subred (220.10.8.63 por ejemplo)

Broadcast: hay dos tipos.

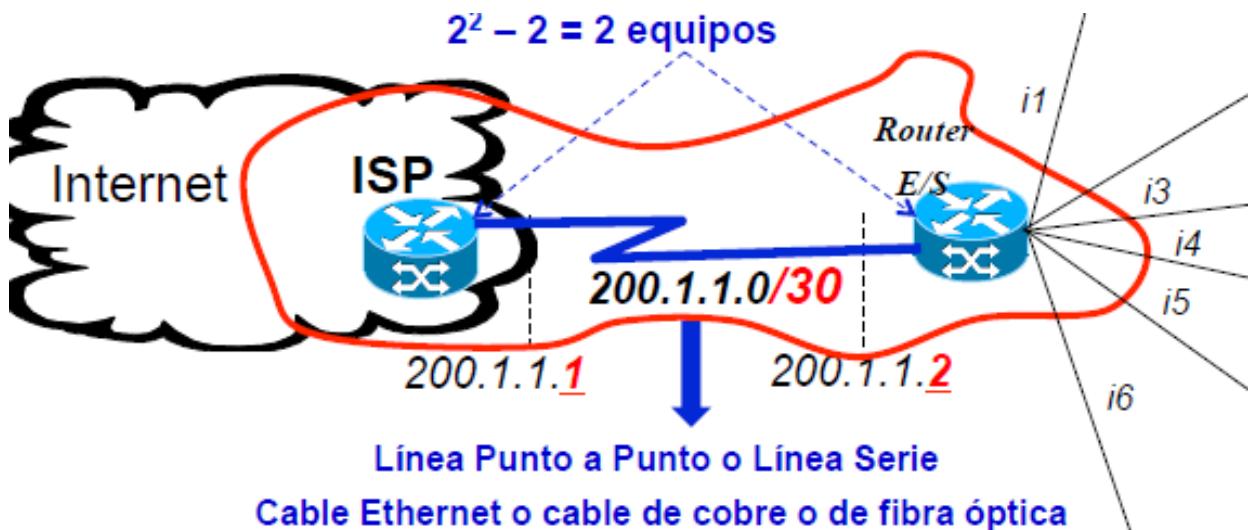
- ❖ **Difusión limitada:** a todos los vecinos de la red o subred local mediante un solo envío desde el equipo de origen. Se señala con la dirección destino 255.255.255.255. Una red de difusión (ethernet o WiFi) es aquella que permite broadcast en el nivel de trama. La dirección MAC destino será también todo a 1, es decir, FF-FF-FF-FF-FF-FF.
- ❖ **Difusión dirigida:** a todos los vecinos de la red o subred local o a todos los equipos de una red o subred remota. La dirección destino se indica poniendo a 1 todos los bits de la parte máquina de la dirección IP. La dirección MAC destino también tiene todos los bits a 1. En una difusión hacia una red o subred remota el paquete IP viaja como una dirección unicast hasta llegar a la red destino, donde el router lo difunde como si fuera 255.255.255.255.

Encaminamiento: hay tres tipos.

- ❖ **Directo:** cuando la máquina destino es vecina. La dirección de red de dicha máquina está registrada en la tabla IP. No hay que pasar por un router vecino.
- ❖ **Indirecto:** cuando la máquina destino no es vecina. La dirección de red de dicha máquina está registrada en la tabla IP. Hay que pasar por un router vecino.
- ❖ **Por omisión:** cuando la máquina destino no es vecina y su dirección de red no está registrada en la tabla IP. Hay que pasar por un router vecino.

Una máquina puede saber si la máquina destinataria es vecina comparando sus direcciones de red.

Enlace punto a punto: red formada por dos equipos (generalmente routers) unidos por enlace ethernet. Por definición la máscara de la red será /30 (255.255.255.252) porque solo puede haber dos equipos.



Máscaras según longitud:

- ❖ **Fija:** máscaras comunes para todas las subredes creadas y por tanto asignan un mismo número de máximos de máquinas a cada subred.
- ❖ **Variable:** máscaras diferentes para las subredes creadas en función de un diferente número máximo de máquinas a cada subred. Se busca el objetivo de usar el menor número de direcciones IP.
 - **Ej.:** se quiere asignar a tres subredes 14, 14 y 30 máquinas respectivamente. La IP de la red que las engloba es 220.10.15.0/25.
 1. El primer paso es ordenar las subredes de mayor a menor tamaño o viceversa (preferiblemente de mayor a menor porque genera menos huecos). En este caso ordenamos de menor a mayor.
 - Subred1: máximo 14 máquinas + router = 15 máquinas
 - Subred2: máximo 14 máquinas + router = 15 máquinas
 - Subred3: máximo 30 máquinas + router = 31 máquinas
 2. Se asigna a la primera subred la dirección IP original 220.10.15.0.
 3. Se calcula la máscara asociada a dicha dirección en función del número máximo de equipos de la subred. Necesitando conectar 15 equipos y tener 2 direcciones reservadas la máscara será /27. Se le asocia la dirección 220.10.15.0/27.
 4. Numeramos las máquinas hasta la difusión dirigida (todo 1s en la parte local de la dirección) 220.10.15.31/27. Nuestro número máximo de máquinas no será exactamente el pedido, sino que será la primera potencia de 2 mayor que el número de máquinas pedido.
 5. Para las siguientes subredes la máscara será /27 y /26 por su número de máquinas. Se les asocia una dirección IP a partir de la difusión dirigida de la anterior subred.
 - Para la subred 2 la dirección será 220.10.15.32/27 y su difusión 220.10.15.63/27.
 - Para la subred 3 la dirección será 220.10.15.64/26 y su difusión 220.10.15.127/26.

Ámbito de aplicación de una dirección IPv4:

- ❖ **Públicas:** las direcciones son públicas y tiene un coste económico adquirirlas.
- ❖ **Privadas:** las direcciones son compartidas y no tienen coste económico. No se usan para salir a Internet, sino que se utilizan únicamente en la red local.

NAT (o NAPT): es un proceso (no un protocolo) que se ejecuta en el nivel de red de E/S del router (es decir, solamente en el router que comunica con Internet) para efectuar dos traducciones:

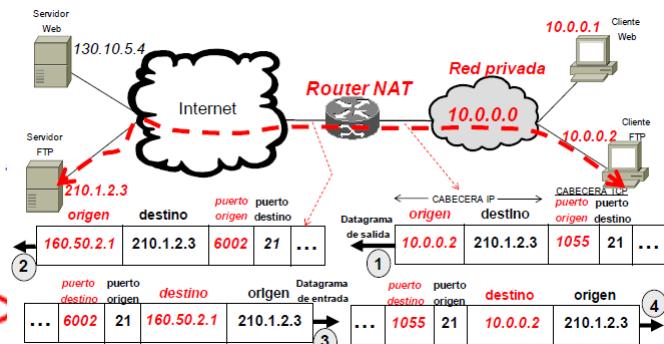
- ❖ Traducción de direcciones entre las IP privadas y las IP públicas.
- ❖ Traducción de números de puerto entre números de puerto privados y números de puerto públicos.

Tiene como objetivo no agotar el espacio oficial de direcciones IP públicas asignables, minimizar su coste y asegurar que no haya un acceso directo desde Internet a la dirección real de un equipo.

Direcciones de clase A, B y C privadas que todo el mundo puede usar y compartir:

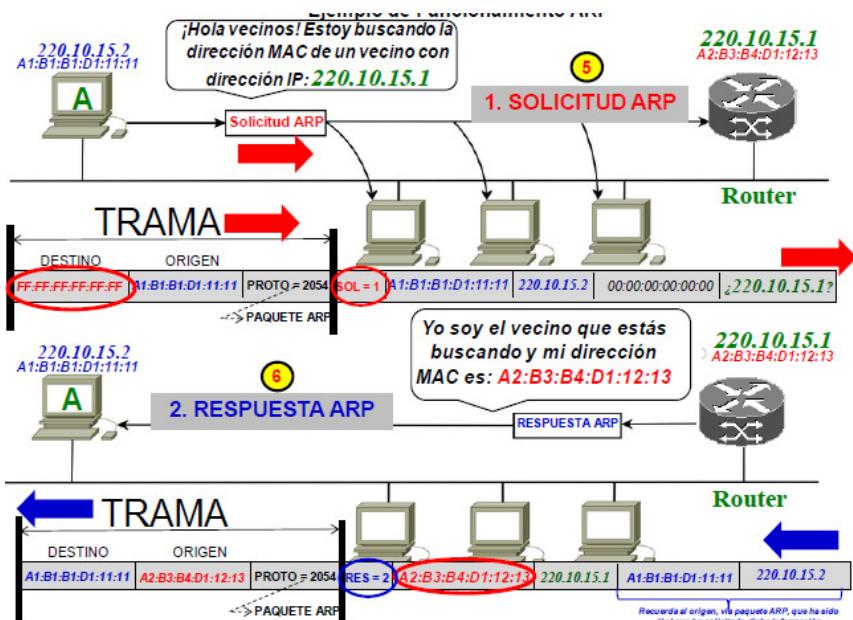
- ❖ Clase A: de 10.0.0.0 hasta 10.255.255.255 (una dirección)
- ❖ Clase B: de 172.16.0.0 hasta 172.32.255.255 (16 direcciones contiguas)
- ❖ Clase C: de 192.168.0.0 hasta 192.168.255.255 (256 direcciones contiguas)

TABLA DE TRADUCCIÓN NAT	
DIRECCIONES PÚBLICAS Y PUERTOS DE LA ORGANIZACIÓN	DIRECCIONES PRIVADAS Y PUERTOS DE LA ORGANIZACIÓN
160.50.2.1:6001	10.0.0.1:2001
160.50.2.1:6002	10.0.0.2:1055

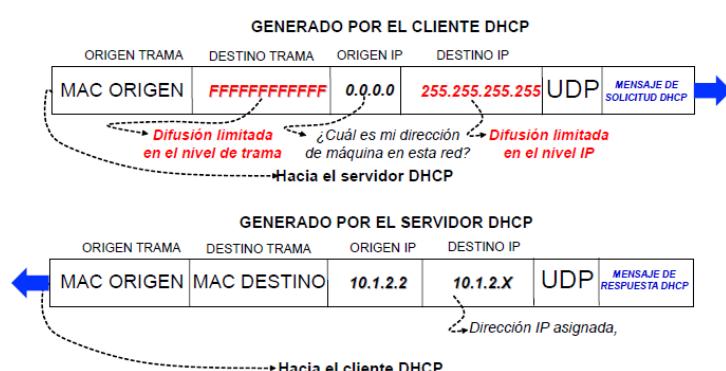


Protocolos y niveles TCP/IP relacionados con el direccionamiento a IP:

- ❖ **ARP (Address Resolution Protocol):** su objetivo es obtener automáticamente la dirección MAC de un equipo vecino. A medida que un equipo se comunica con equipos vecinos su entidad ARP va gestionando una tabla ARP que relaciona direcciones IP con direcciones MAC. Cuando pasa un determinado tiempo de actividad (p. ej. 15 minutos) o se apaga el equipo se pierde toda la información, que el protocolo ARP volverá a recolectar según se vaya conectando a otras máquinas. Así se evita que el administrador tenga que gestionar altas y bajas puntuales.

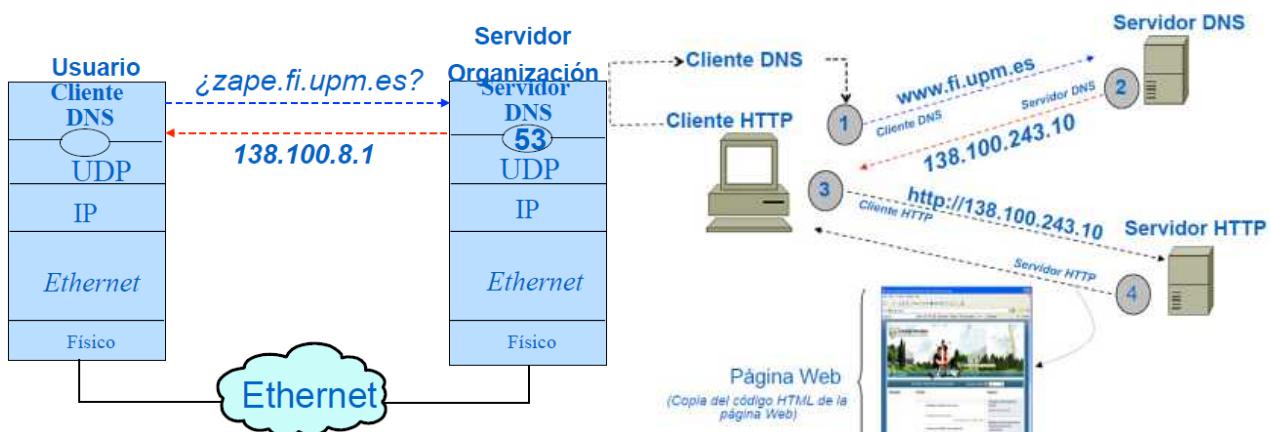


- ❖ **DHCP:** se ejecuta en el nivel de aplicación sobre UDP. Se usa solo entre equipos vecinos. En equipos de usuario se monta con el número de puerto 68 y en routers E/S con el puerto 67. Cuando el equipo se conecta a una red que no conoce manda por broadcast un paquete IP con un mensaje de solicitud DHCP para recibir una IP asignada y demás información de configuración.



- ❖ **DNS (Domain Name System):** se ejecuta en el nivel de aplicación y se monta sobre UDP, ya que son mensajes cortos y los servidores DNS se suelen encontrar en redes Ethernet, que son fiables. A diferencia de DHCP y ARP que necesitan comunicarse con equipos vecinos, un servidor DNS puede estar disperso en Internet porque el acceso al equipo servidor nunca se da por broadcast sino por la dirección IP de dicho equipo.

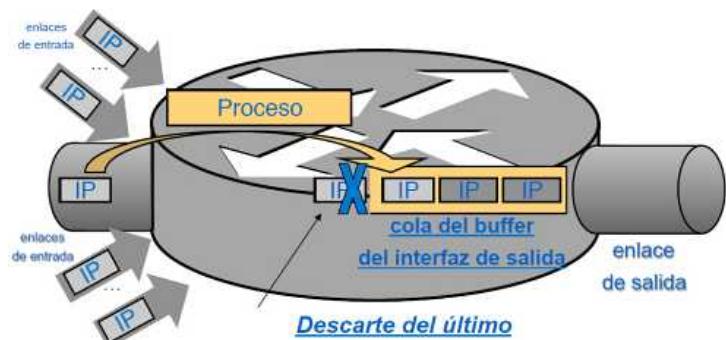
- Aparte de su dirección IP (dirección numérica), un equipo que ofrezca procesos servidores en Internet puede disponer también de una dirección simbólica para que los potenciales usuarios puedan indicar una dirección IP por el formato simbólico asociado.



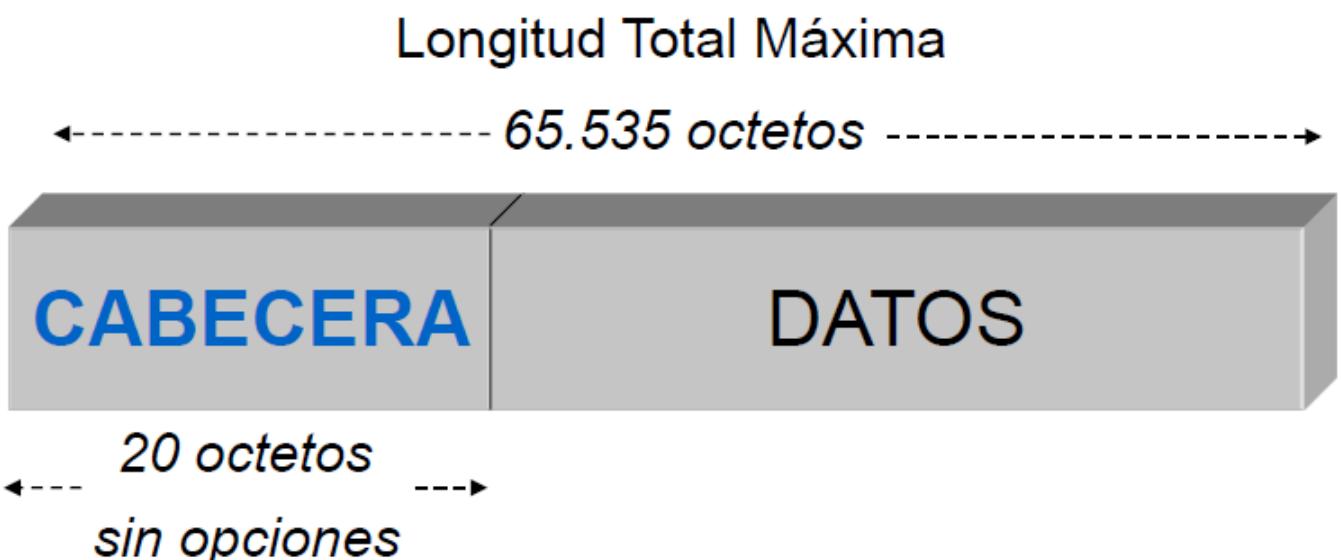
Composición de paquetes IPv4:

Todos los mensajes de todos los protocolos del nivel de aplicación se encapsulan siempre en paquetes IP para un encaminamiento rápido (sin fiabilidad) entre equipos vecinos por Internet.

Uno de los principales problemas en Internet es la congestión en los routers de núcleo. Si un paquete IP no se puede encaminar o genera un problema a una entidad IP, esa entidad tira el paquete a la basura. Uno de esos problemas es que se desborde la capacidad de almacenamiento de los buffers asociados a las distintas líneas de código.



El paquete IP se divide como se muestra en la próxima imagen. Aunque la longitud máxima teórica es 65.535 bytes en la práctica no puede ser superior a 1500 bytes ya que es el tamaño de la MTU (Maximum Transfer Unit) de salida, es decir la longitud máxima del campo de datos de una trama Ethernet.

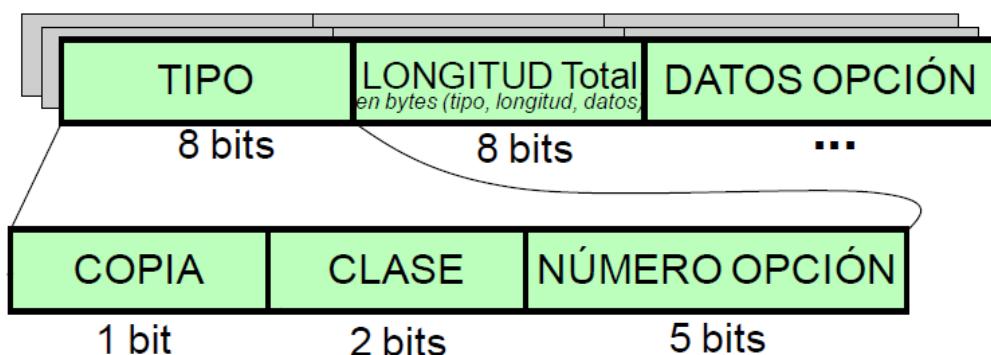


Longitud práctica en función de la MTU de salida = 1500 bytes

La cabecera de un paquete IP se divide de la siguiente manera:



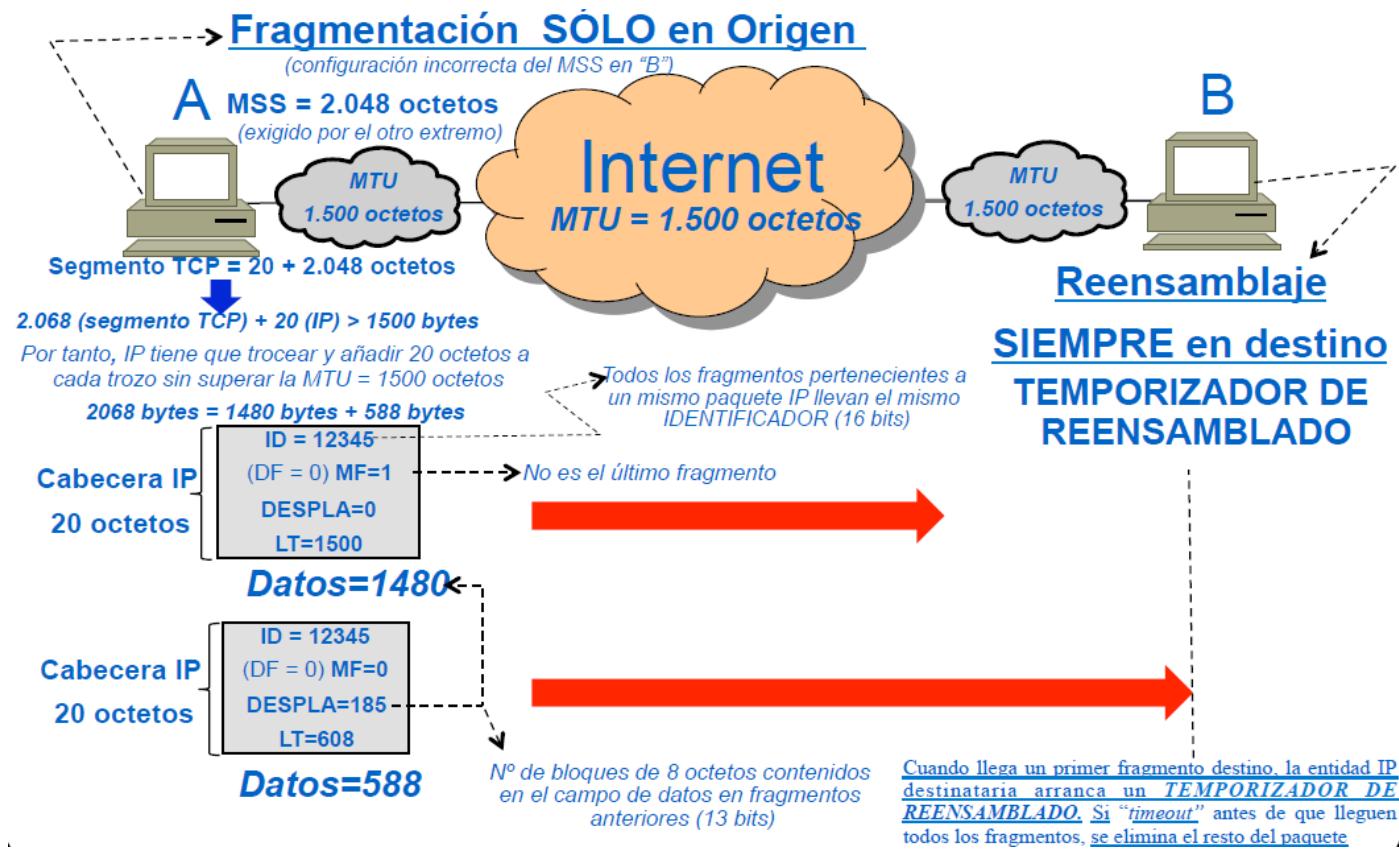
- ❖ Versión: IPv4
- ❖ Longitud de cabecera: puede tener un tamaño variable según haya más o menos opciones después de las direcciones.
- ❖ Tipo de servicio: refleja la calidad de servicio que se ofrece al paquete. Depende del servicio contratado por el usuario a su operador.
- ❖ Longitud: indica la longitud total en bytes del paquete IP.
- ❖ Identificador: marca con el mismo valor a todos los fragmentos de un mismo paquete.
- ❖ MF: more fragments, indica si a continuación hay más fragmentos del paquete. Si es el último vale 0.
- ❖ Desplazamiento: número de bloques de 8 bytes contenidos en el campo datos de fragmentos anteriores.
- ❖ DF: bit de no fragmentar, si está activado el paquete IP no debe ser fragmentado.
- ❖ Tiempo de vida: número de routers por los que puede pasar el paquete. Un paquete no puede atravesar más de 255 routers. Cada router reduce en 1 el valor de este campo. Si el resultado es 0 se elimina el paquete IP. Así se evitan viajes en bucle.
- ❖ Protocolo: según lo que se esté transportando para que la entidad IP del equipo destinatario sepa a qué protocolo llamar.
- ❖ Suma de comprobación: suma aritmética binaria sin acarreo de todos los bloques de 16 bits de los que consta la cabecera. Aunque IP sea no fiable detecta posibles fallos físicos en la cabecera. Si se detecta alguno se tira el paquete IP a la basura.
- ❖ Opciones: campo de longitud variable para solicitar servicios adicionales. Si no hay ninguna opción la cabecera es de 20 bytes, siendo su tamaño máximo 60 bytes.
 - Formato TLV: Tipo, Longitud Valor. El campo tipo se subdivide en:
 - Copia: indica si la opción se debe copiar en todos los fragmentos en los que se divide el paquete o solo en el primero.
 - Clase: 0
 - Número de opción: determina como se interpreta el campo Datos Opción de la imagen siguiente.
 - Encaminamiento desde origen: estricto (cada entidad IP intermedia quita su dirección IP y encamina a la siguiente de la lista) o no estricto.
 - Registro de ruta: identificación IP de cada router
 - Sello de tiempo: identificación IP de un router y del momento en que dicho router procesa el datagrama.



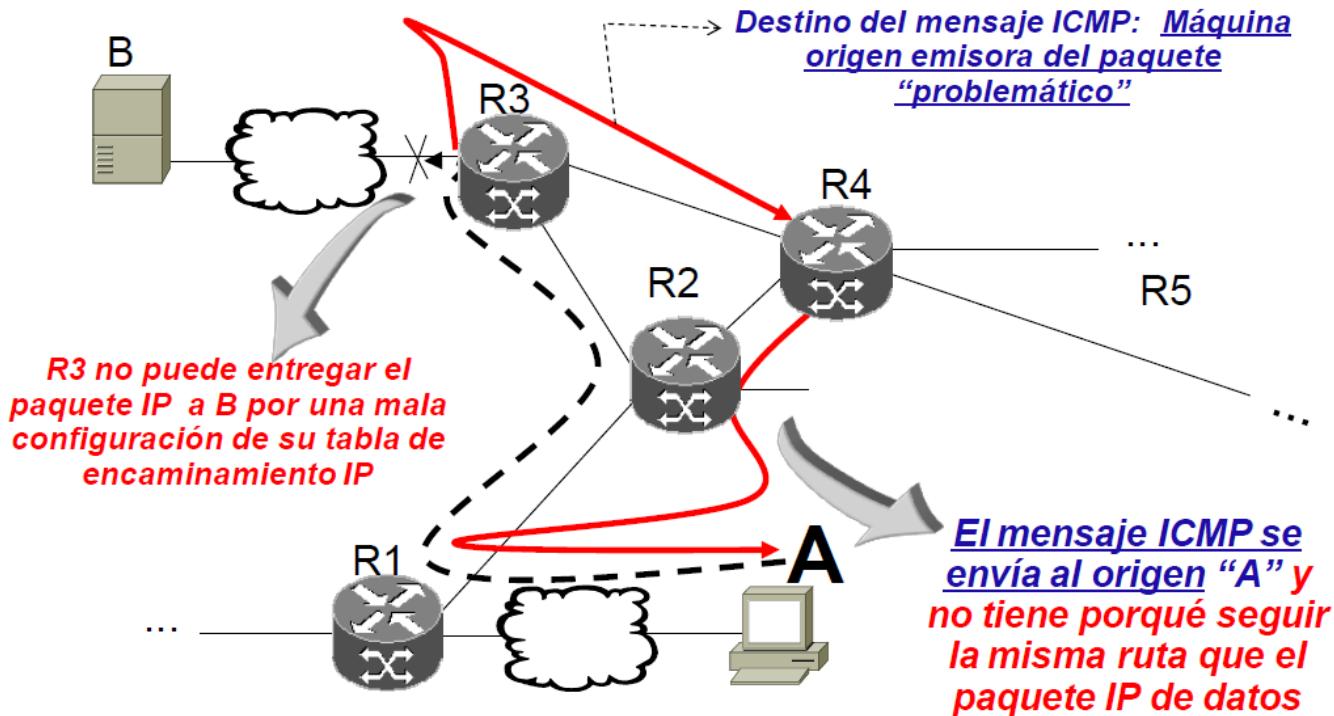
Rutina de comprobación de la cabecera IP:

1. Suma de Comprobación
2. Versión
3. Longitud de Cabecera
4. Longitud Total
5. Decrementar TTL
 - ✓ Solo las entidades IP intermedias, no las de origen ni destino.
 - ✓ Si el resultado es 0 se elimina el paquete.
 - ✓ Se calcula y actualiza la suma de comprobación.

Fragmentación de un paquete IP: se realiza cuando el tamaño de un paquete IP es superior a 1500 bytes, la longitud de la MTU. Se debe evitar en la medida de lo posible porque aumenta la carga de tráfico y de proceso, así como la posibilidad de perder un datagrama IP. Solo se fragmenta en el equipo origen.



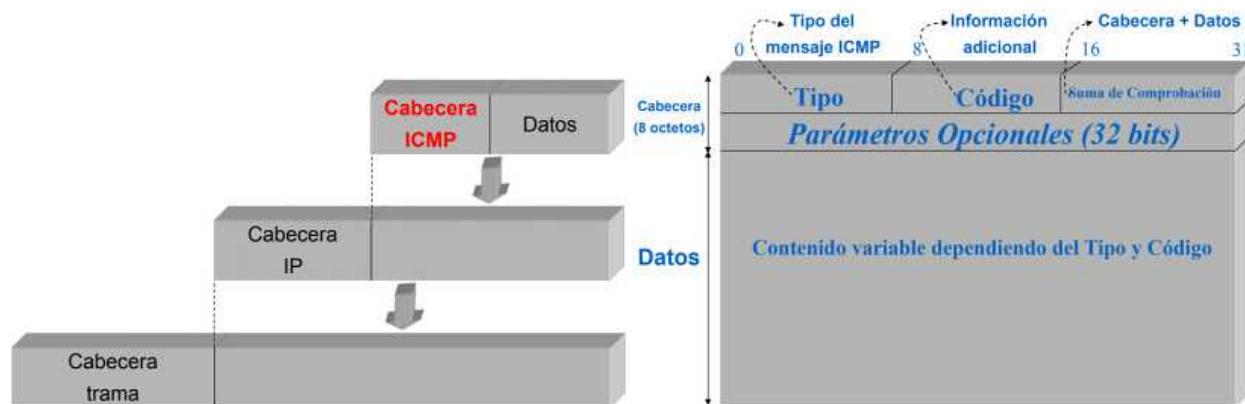
Protocolo ICMP: es el protocolo de envío de mensajes de control en Internet. Ocupa un subnivel superior al protocolo IP dentro del nivel de red, ya que todo mensaje ICMP se encapsula en un paquete IP. Notifica fallos relacionados con el encaminamiento del paquete IP a la máquina origen emisora del paquete IP problemático. ICMP no hace más fiable a IP.



Tipos de mensajes ICMP:

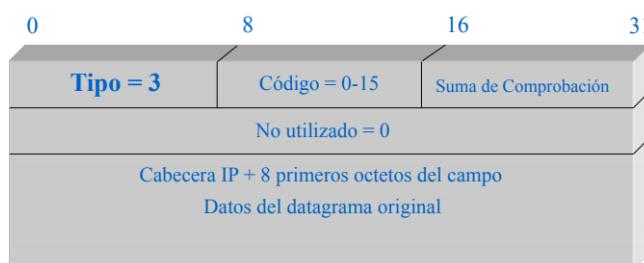
- ❖ **Informes de fallos:** Problemas que un router, o la máquina destino (o, incluso, la máquina origen), pueden encontrar al procesar un datagrama IP
 - Destino inalcanzable (falta de información en la tabla IP)
 - Tiempo excedido (TTL = 0 en un router o tiempo de reensamblado excedido en la máquina destino)
 - Problemas con los parámetros (información ininteligible en la cabecera del datagrama IP)
 - Etc.
- ❖ **Consultas:** Información que permite que una máquina tenga datos de otra
 - Solicitud y respuesta de eco (comprobación de si una máquina está conectada y responde)
 - Etc.

Encapsulación y formato ICMP: el tamaño máximo viene condicionado por el tamaño máximo de 1500 bytes del paquete IP, restándole a eso los 20 bytes de cabecera. Por tanto, el mayor tamaño posible de una cabecera ICMP sería de 1480 bytes con un campo de datos de 1472 bytes.



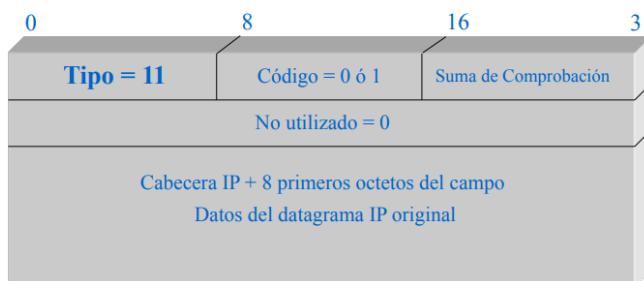
- ❖ **Destino inalcanzable:** algunos valores del campo de código, que va de 0 a 15, son:

- 0: red no alcanzable
- 1: máquina destinataria no alcanzable o sin respuesta ARP (router final)
- 2: protocolo superior (TCP, UDP, etc.) no alcanzable (nivel de red o IP de la máquina destinataria)
- 3: puerto no alcanzable (nivel de transporte de la máquina destinataria)
- 5: fallo en el encaminamiento desde origen (máquina origen o router)



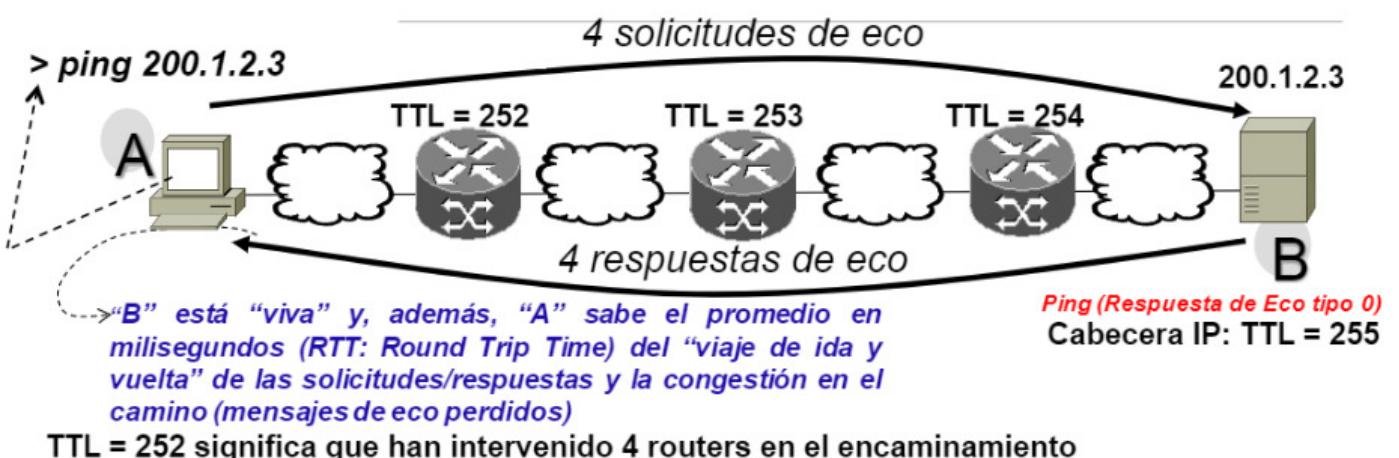
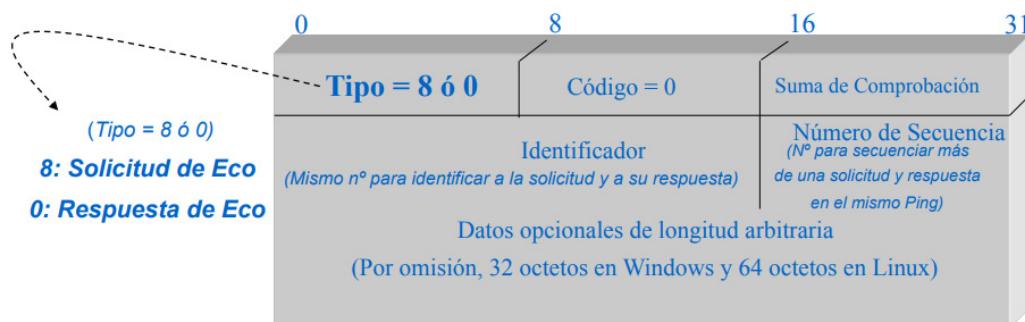
- ❖ **Tiempo excedido:** el campo código puede tomar los valores 0 y 1:

- 0: Tiempo de vida (TTL) del datagrama excedido
- 1: Tiempo de reensamblado excedido



❖ **Solicitud y respuesta de eco (Ping):** el comando ping hace uso de los mensajes ICMP de solicitud y respuesta de eco para saber si un equipo por Internet está conectado y responde. La combinación de ambos mensajes determina si dos equipos se pueden comunicar entre sí por Internet, es decir, si hay comunicación en el nivel IP. Si se envía un mensaje de solicitud de eco y se recibe un mensaje de respuesta “con el mismo eco” es que hay comunicación IP con el equipo destino y, además, los routers intermedios están encaminados. Los usos del comando ping son:

- Saber si un equipo en Internet está conectado
- Conocer el número de mensajes ICMP enviados, recibidos y perdidos por el camino
 - Si hay perdidas de mensajes ICMP seguramente hay congestiones en algún router en el trayecto por Internet
- Calcular el tiempo aproximado (RTT: Round Trip Time), mínimo, máximo y promedio, de ida y vuelta de las solicitudes y correspondientes respuestas ICMP
- Conocer el número de routers entre el origen y destino mediante el decremento del TTL en la cabecera IP
- Obtener la dirección IP asociada a una dirección simbólica



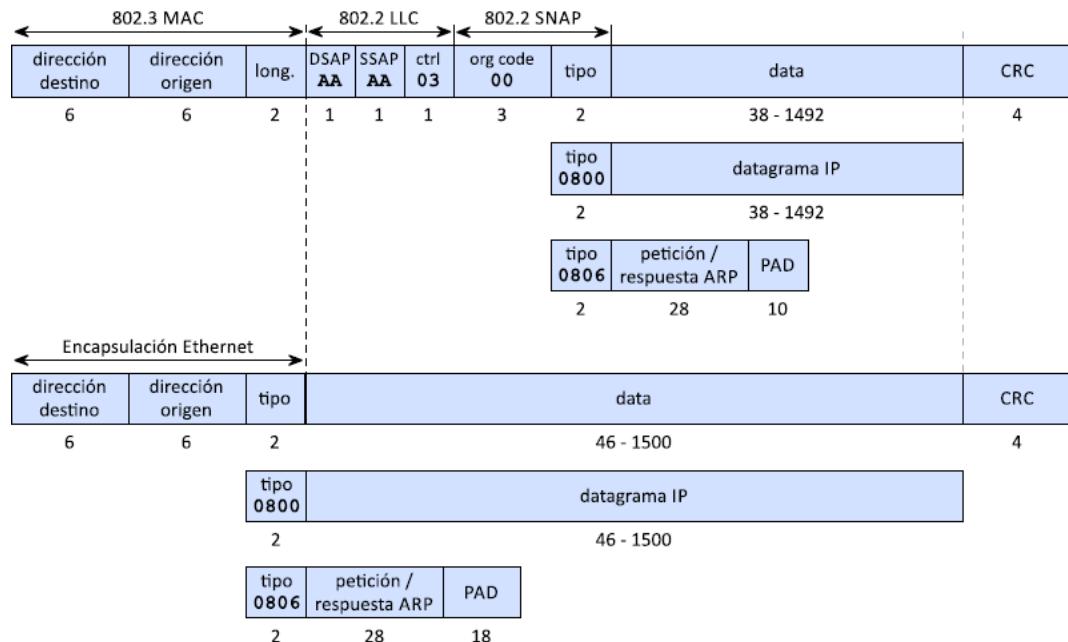
3. TECNOLOGÍAS DE REDES DE ÁREA LOCAL

3.1 ETHERNET

Ethernet es la tecnología LAN más utilizada. Incluye nivel de enlace y nivel físico. Se corresponde con una familia de tecnologías definidas en los estándares Ethernet II e IEEE 802.2 y 802.3.

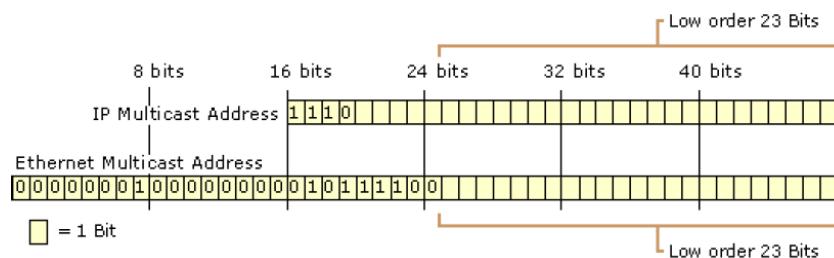
7 Octetos	1 Oct.	6 Oct.	6 Oct.	2 Oct.	0 a 1.500 Oct.	4 Oct.	
Preámbulo	SFD	Dirección destino	Dirección origen	Long. ó Tipo	LLC y/o Datos	Relleno 0 - 46	SVT

- ❖ **Preámbulo:** para sincronización, encabezan 7 octetos con el patrón 10101010.
 - ❖ **SFD (Start Frame Delimiter):** delimitador de comienzo de trama 10101011.
 - ❖ **MAC destino**
 - ❖ **MAC origen**
 - ❖ **Longitud (IEEE 802.3) o Tipo (Ethernet II):** el tipo o Ethertype es el protocolo de nivel superior.
 - ❖ **LLC (IEEE 802.3) y/o Datos (Ethernet II):** los datos en Ethernet II son la IP
 - ❖ **Relleno:** para alcanzar la longitud mínima de trama de 64B (sin incluir el preámbulo ni el SFD).
 - ❖ **SVT (Secuencia de Verificación de Trama)**



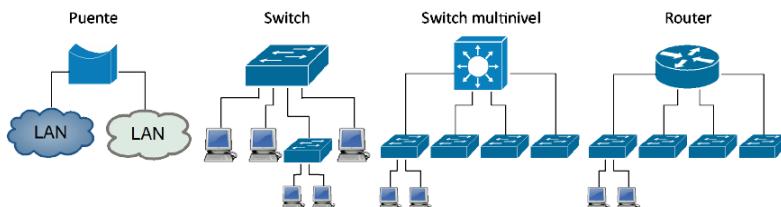
Si se transmite una trama menor o mayor que los tamaños mínimo y máximo el dispositivo la descarta. Existen tramas con tamaño mayor que el estándar, como las Jumbo (9000B) y las Baby Jumbo (4B extra con información de la VLAN).

MAC: para soportar IP multicast se han reservado el rango de direcciones Ethernet de 01-00-5E-00-00-00 a 01-00-5E-7F-FF-FF. Los últimos 23 bits de la dirección IP se mapean en los últimos 23 bits de la dirección Ethernet. Hay 5 bits de la IP multicast que no se mapean, por lo que varias IP multicast se mapean a la misma Ethernet multicast

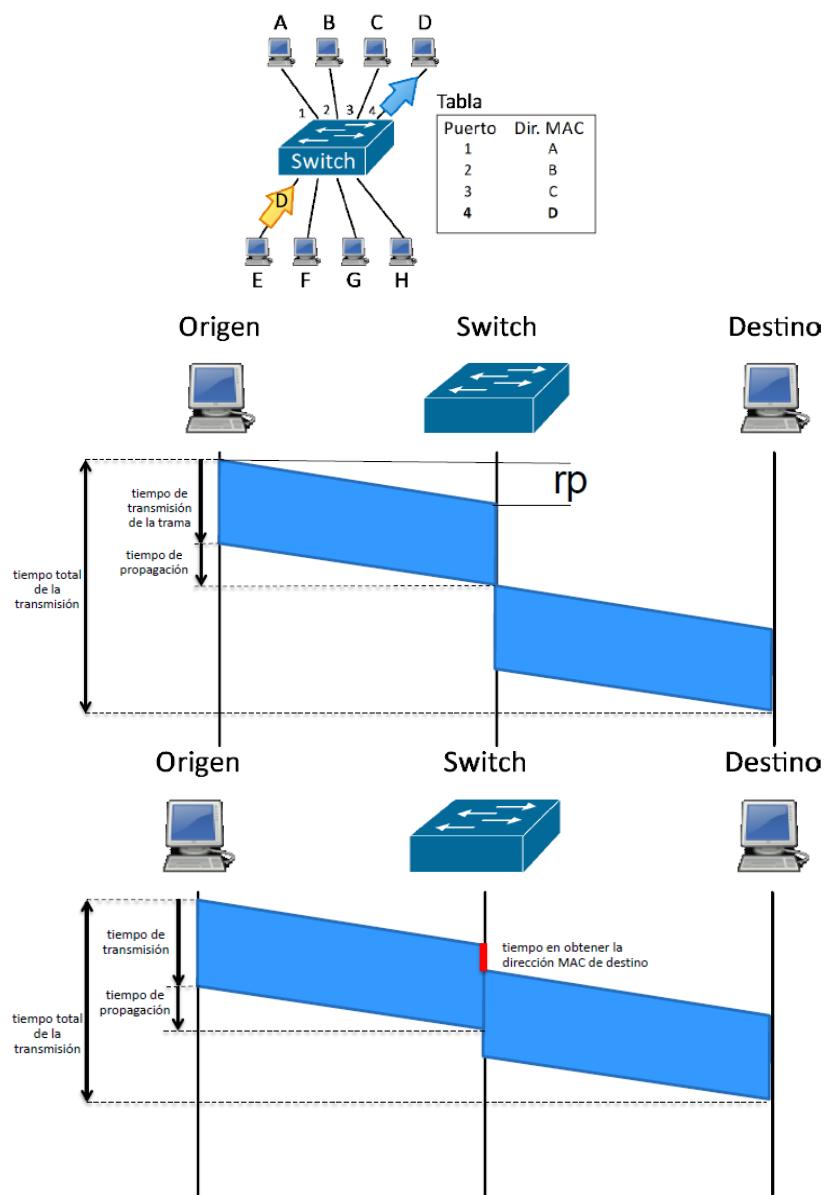


Dispositivos de interconexión: conectan entre sí los diferentes elementos de red, creando redes de área local. Permiten segmentar una LAN, creando varios dominios de colisión:

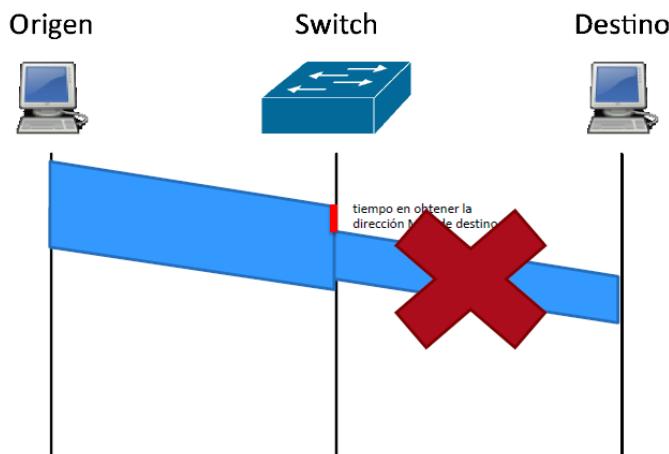
- ❖ Extienden el rango de una LAN de forma transparente
- ❖ Las LAN no tienen por qué ser del mismo tipo
 - Punto de acceso WiFi: Puente WiFi <-> Ethernet
- ❖ Almacenan temporalmente las tramas
- ❖ Retransmiten en base a la dirección MAC de destino
- ❖ No disponen de funcionalidad de control de flujo



Switch: es un puente multipuerto que permite comunicaciones simultáneas, separando dominios de colisión. No necesita configuración. Aprende las MAC de cada estación conectada a cada puerto, construye las tablas de conmutación en base a dichas MAC y si no conoce una MAC difunde la trama por todos los puertos excepto por el que ha llegado. Usan dos técnicas de conmutación: almacenamiento y retransmisión (Store and Forward) y Cut-through.



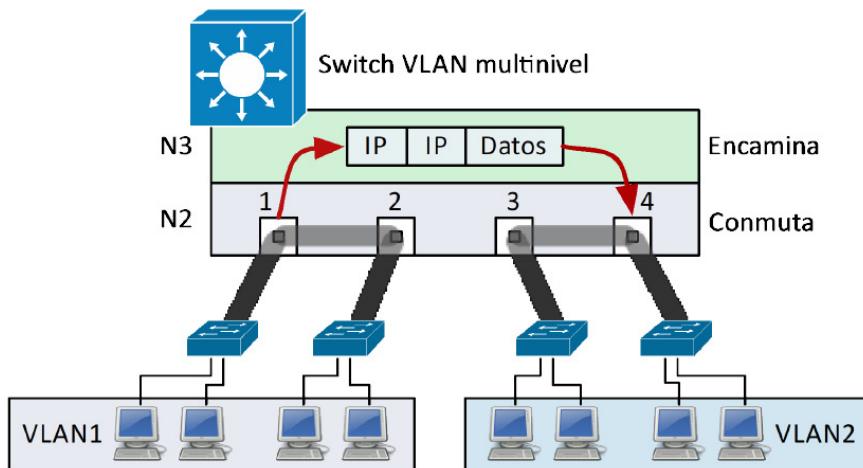
Los switches permiten conectar dispositivos a diferente velocidad. No se puede utilizar cut-through hacia puertos más rápidos que el de recepción



Los switches no limitan el dominio de difusión. Sin embargo, son susceptibles a bucles, por lo que es necesario utilizar mecanismos que los eviten como el STP (spanning tree protocol).

Switch multinivel: añan funciones de los switches y los routers, realizando las de los segundos a nivel de hardware, que es más rápido.

- ❖ Nivel 2: conmuta a partir de la dirección MAC, como cualquier otro switch
- ❖ Nivel 3: conmuta a partir de la MAC dentro de una misma VLAN. Incluye funcionalidad de nivel 3 (encaminamiento, filtrado, multicast, etc.)
- ❖ Nivel 4: filtra el tráfico analizando los puertos TCP/UDP

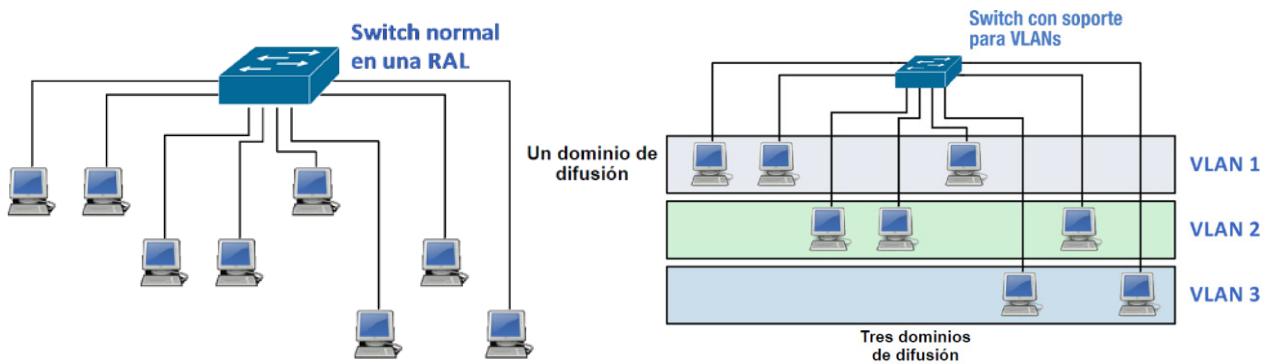


Trama PAUSE: solamente se puede utilizar en estaciones dúplex. Cuando el dispositivo estima que se ha superado un umbral de ocupación de buffers, emite la trama PAUSE al dispositivo par implicado en la comunicación. La MAC destino será 01:80:C2:00:00:01 y los parámetros incluyen un valor que especifica el tiempo durante el cual el emisor debe cancelar la transmisión de más tramas de datos.

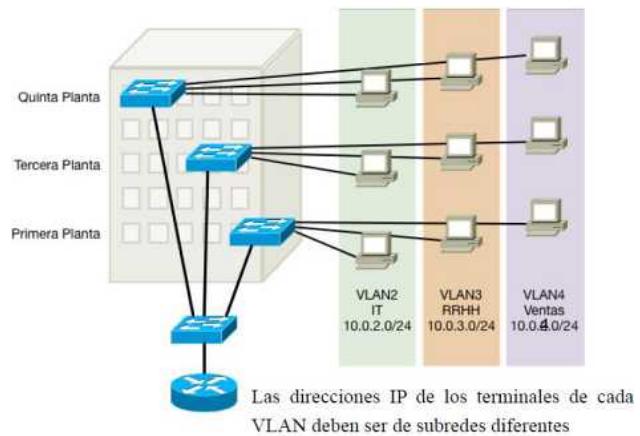
Preámbulo	SFD	MAC destino 01:80:C2:00:00:01	MAC origen	tipo 0x8808	Opcode 0x0001	Params	Reserved	SVT
Bytes	7	1	6	6	2	2	42	4

Autonegociación: puede ocurrir que los dos dispositivos implicados en una comunicación no soporten las mismas opciones. IEEE 802.3 define un mecanismo para que los dos extremos se pongan de acuerdo. La autonegociación también optimiza la labor de instalación de las LANs anulando posibles errores humanos. El proceso de autonegociación lo realiza el nivel físico y tiene lugar al arrancar los dispositivos.

3.2 REDES DE ÁREA LOCAL VIRTUALES (VLANs)



Una red de área local virtual es una partición de una red física de nivel 2. Dicha partición tiene lugar en los switches. Cada VLAN se corresponde con un dominio de broadcast. Las VLANs están aisladas unas de otras a nivel 2, por lo que los paquetes destinados a una VLAN deben llegar a través de un dispositivo con funcionalidad de nivel 3. Los equipos agrupados en una VLAN no son conscientes de la existencia de dicha VLAN.

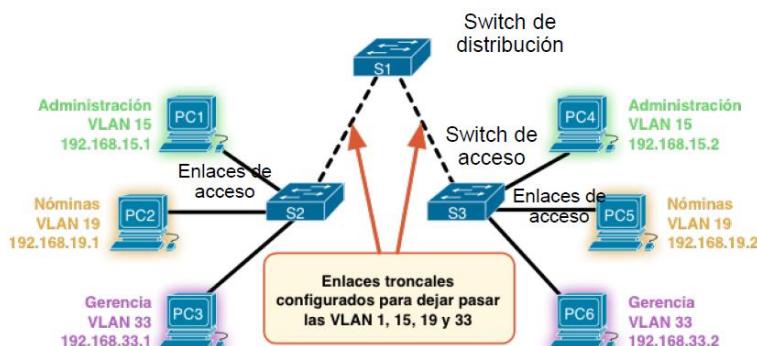


Tipos de VLANs:

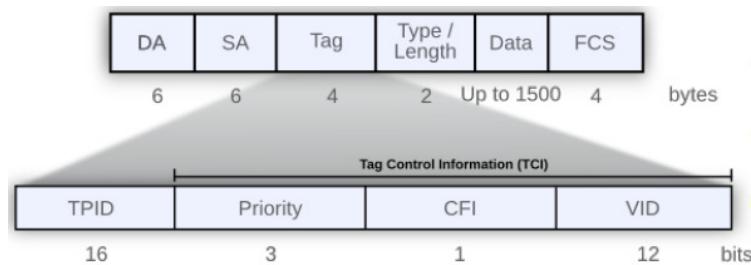
- ❖ **VLAN por defecto:** a la que pertenecen los puertos de un switch cuando no están asignados a ninguna otra VLAN.
- ❖ **VLAN de gestión y administración:** necesita IP por la que acceder a gestionar y administrar VLANs.
- ❖ **VLAN de datos:** dedicadas a transmitir el tráfico generado por los usuarios.
- ❖ **VLAN de voz:** para el tráfico de datos de voz.

Las VLANs se identifican por el puerto de conexión al switch, por la dirección IP y por etiqueta 802.1Q (tramas baby jumbo).

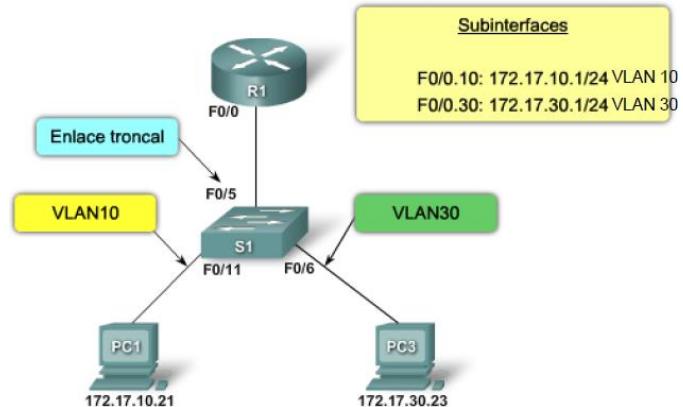
Enlaces troncales: son aquellos que pueden llevar datos de más de una VLAN. Se establecen típicamente entre switches, por lo que dispositivos pertenecientes a la misma VLAN pueden comunicarse a nivel 2 incluso cuando están conectados físicamente a diferentes switches. Un enlace troncal no está asociado a una VLAN concreta. El protocolo de enlaces troncales más popular es IEEE 802.1Q.



Las estaciones envían y reciben tramas Ethernet normales. Los switches insertan la etiqueta 802.1Q (4B) añadiendo un campo adicional a la trama Ethernet y la retiran antes de entregar la trama a la estación de destino.



Subinterfaces: son interfaces virtuales asignadas a una interfaz física. Cada subinterfaz se configura con su propia dirección IP, máscara de subred y asignación de VLAN única.

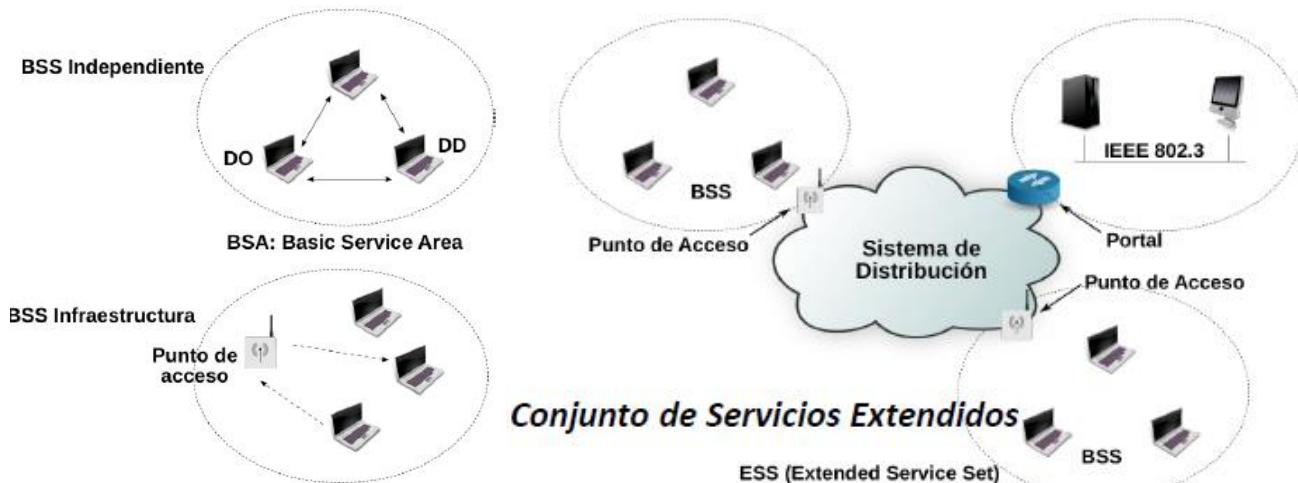


3.3 REDES INALÁMBRICAS (Wi-Fi)

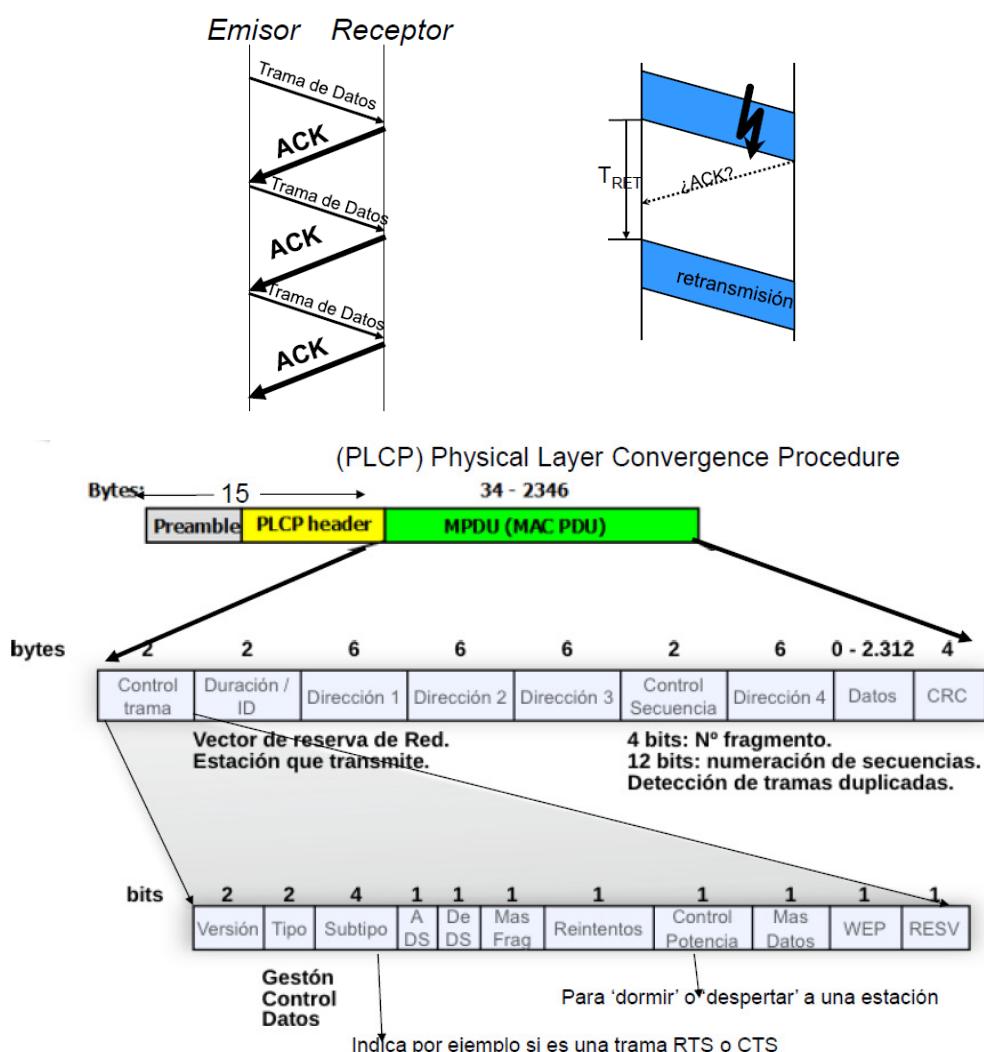
Redes independientes: comunicación directa entre terminales.

Redes de infraestructura: la comunicación entre terminales se hace a través del punto de acceso.

Redes extendidas: un punto de acceso se comunica con otro punto de acceso.



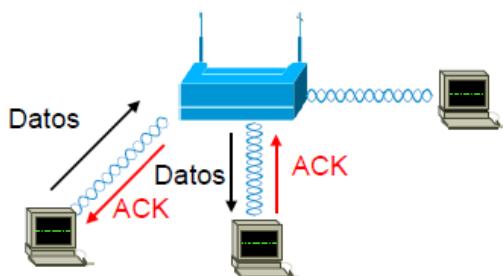
La entidad emisora, una vez transmitida una trama, se para y espera a recibir su confirmación antes de enviar una nueva trama. Al vencimiento del temporizador, si no se recibe validación, se transmite la trama. La entidad receptora transmite un ACK si la trama se ha recibido correctamente.



BSS (Basic Service Set): no tienen punto de acceso y suelen ser temporales. Todo BSS se identifica por un SSID (cadena de texto que identifica la red) y un BSSID (MAC generada aleatoriamente que hace de punto de acceso).



BSS-I (Basic Service Set Infraestructure): contiene una o más estaciones inalámbricas y una estación central que se denomina punto de acceso. No se comunican entre ellas directamente, sino a través del punto de acceso. Todo BSS-I se identifica por un SSID (cadena de texto que identifica la red) y un BSSID (MAC de la interfaz WiFi del punto de acceso).



ESS (Extended Service Set): comunica varios BSSs conectados por un sistema de distribución (generalmente Ethernet). Es necesario hacer roaming, es decir, el servicio se desasocia del BSS en el que está y se asocia al nuevo al que se va a conectar. Esto ocurre por ejemplo cuando estamos conectados a la red WiFi de la facultad y nos vamos moviendo físicamente por el campus. Todo BSS se identifica por un SSID (cadena de texto que identifica la red) y un BSSID (cada BSS se identifica con la MAC de la interfaz WiFi de su punto de acceso).

Tipos de tramas:

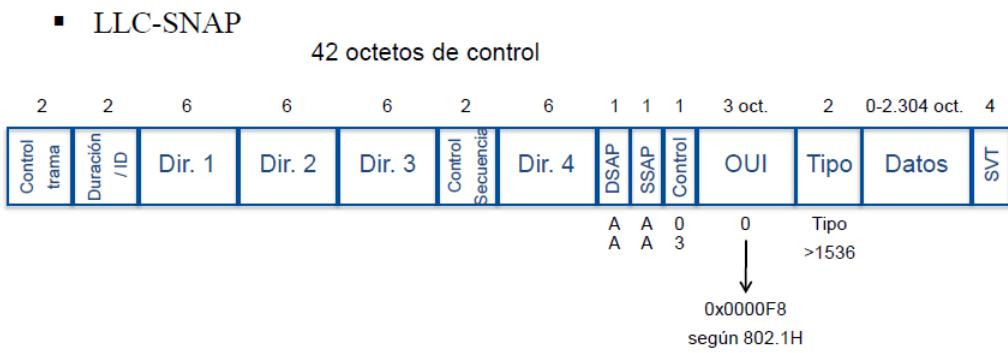
- ❖ **Datos**
- ❖ **Control**
 - **ACK:** validación de trama de datos
 - **RTS (Request To Send):** reserva del canal
 - **CTS (Clear To Send):** validación de la reserva por parte del receptor
- ❖ **Gestión:**
 - **Beacon:** el punto de acceso advierte su presencia transmitiéndolas. Contienen información como el nombre de la red y las capacidades del punto de acceso.
 - **Probe:** permite a una estación preguntar si hay alguna red en un determinado canal
 - **Authenticate:** para autenticación de la estación frente al punto de acceso con una clave que cada terminal comparte con el punto de acceso.
 - **Associate:** para llevar a cabo el proceso de conexión de una estación con el punto de acceso.
 - **Dissociate:** para desconexión de un punto de acceso
 - **Reassociate:** para conectarse a un punto de acceso
 - **Deauthentication**

Trama RTS				
FC	D	Dirección 1	Dirección 2	CRC
bytes	2	2	6	6

Trama CTS o ACK			
FC	D	Dirección 1	CRC
bytes	2	2	4

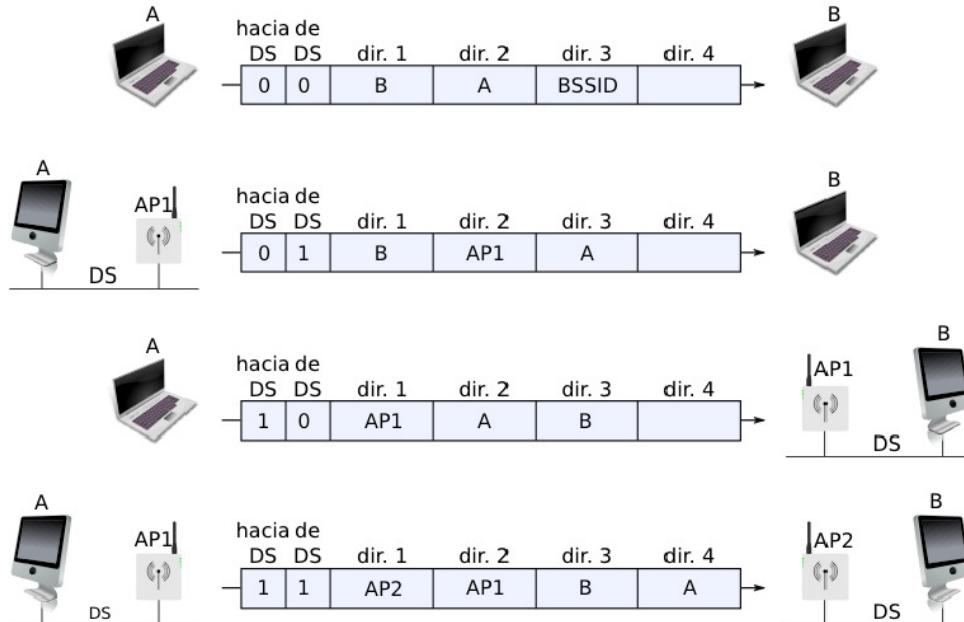
FC: Control trama
D: Duración

Encapsulación IP: IEEE 802.11 –RFC 1042 y IEEE 802.1H



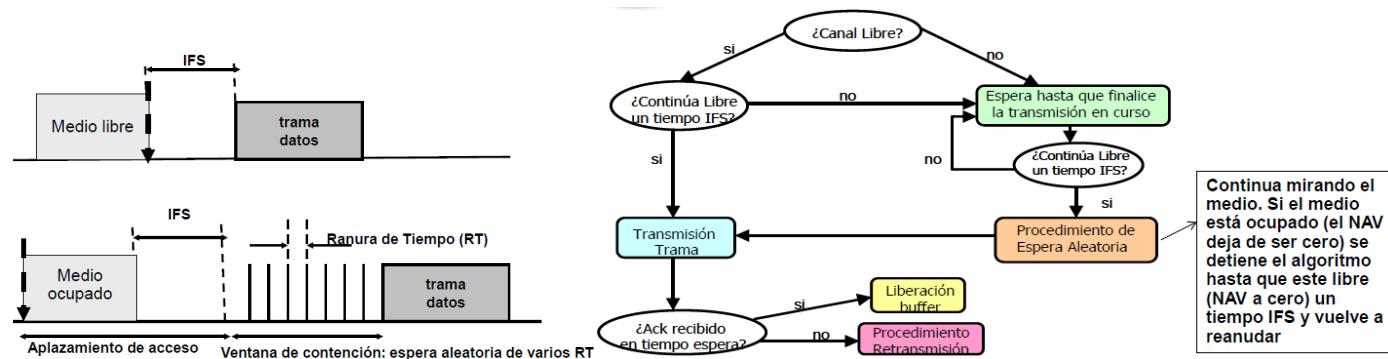
Direcciones MAC: el subnivel MAC utiliza 4 direcciones. Origen y destino (absolutas) y transmisor y receptor (intermedios).

dir 1: Terminal ó PA receptor; dir 2: Terminal ó PA transmisor; dir 3: otro terminal



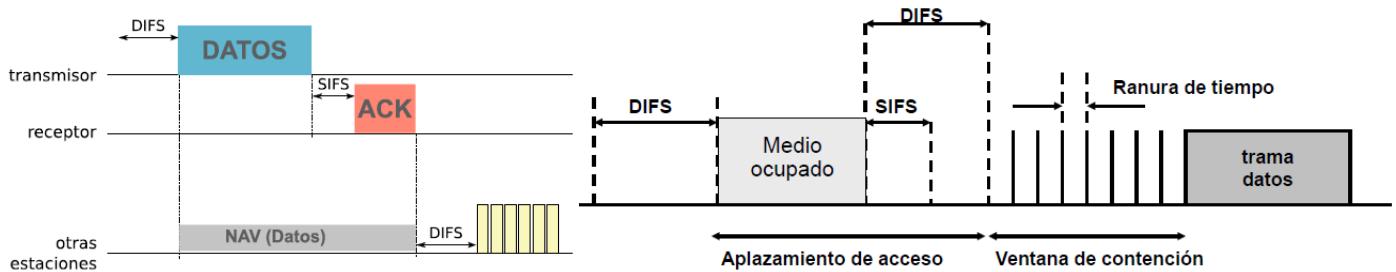
Control de acceso al medio: el proceso CSMA se utiliza para detectar primero si el medio transporta o no una señal. Las estaciones pueden transmitir en cualquier momento. Si no se detecta una señal, el dispositivo transmite sus datos. Si dos dispositivos transmiten a la vez, se produce una colisión de datos.

Función de coordinación distribuida: todas las estaciones deben estar activas durante un periodo mínimo denominado espacio entre tramas (IFS Inter Frame Space). Antes de enviar una trama se espera un IFS. Si está libre durante el IFS se transmite. Si está ocupado se espera a que finalice la transmisión en curso, se espera un IFS y si continúa libre espera un periodo aleatorio y después transmite. Las tramas de confirmación esperan un IFS más corto, de forma que siempre pasarán por delante de cualquier otra comunicación.

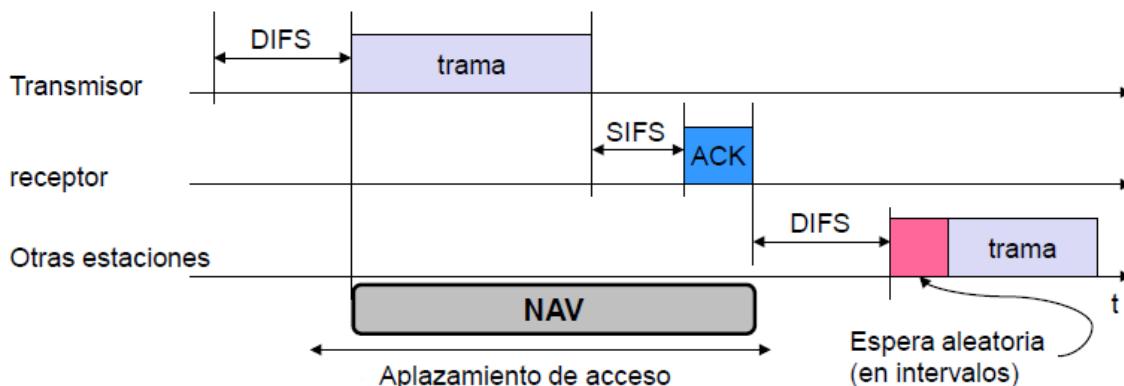


Se utilizan dos IFS diferentes:

- ❖ DIFS: espera obligada para cada estación con intención de transmitir datos
- ❖ SIFS: espera menor para enviar confirmaciones. Tienen mayor prioridad y no esperan ventana de contención. Para ACK, CTS y tramas de datos segmentadas.

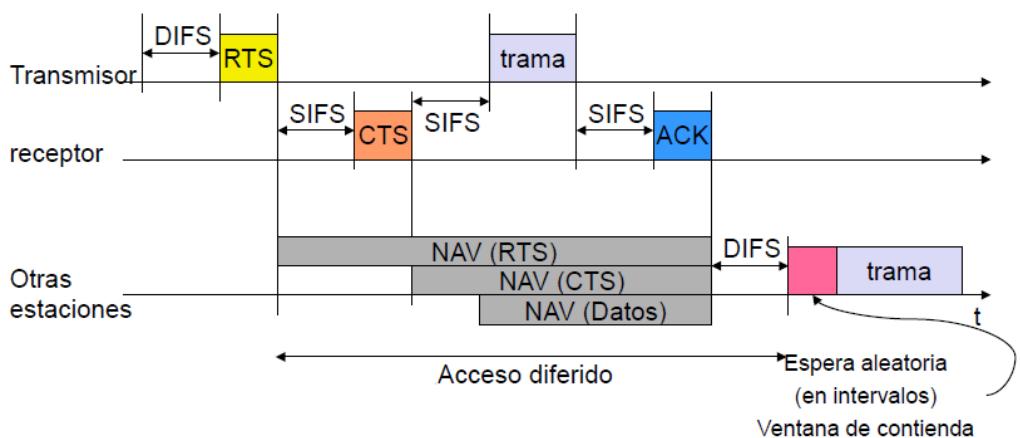


NAV: contador de tiempo que debe pasar para que el canal quede libre. Una estación comprueba el NAV y no intenta transmitir mientras $NAV > 0$. Vuelve a escuchar el canal cuando $NAV = 0$, espera un IFS y transmite si puede.

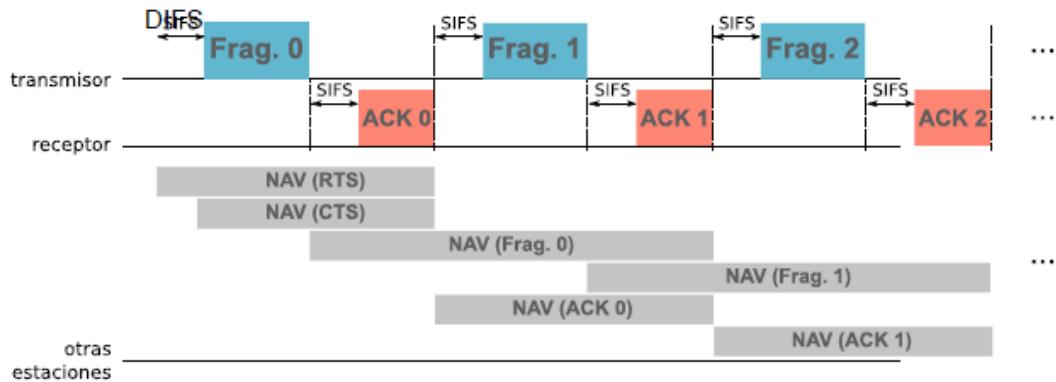


Colisiones:

- ❖ Supongamos que dos estaciones detectan el medio libre y deciden transmitir a la vez. En este caso el riesgo de colisión es mínimo por la gran velocidad de la señal.
- ❖ Supongamos que dos estaciones en espera eligen el mismo número de intervalos para transmitir después de la emisión en curso. En este caso reintentan ampliando exponencialmente el número de intervalos y vuelven a elegir. Es similar a Ethernet salvo que las estaciones no detectan la colisión, deducen que se ha producido cuando no reciben el ACK esperado.
- ❖ Supongamos que dos estaciones no se escuchan la una a la otra, pero si el punto de acceso. Si intentan enviar a la vez ocurre lo mismo que en el caso anterior, aunque existe el mecanismo de reserva RTS-CTS (Request To Send-Clear To Send), útil en casos de mucha congestión o muchos terminales ocultos.
 - RTS: solicitud para transmitir. Lleva información sobre la duración de la trama.
 - CTS: permiso para transmitir y reserva de recursos (NAV) para todas las estaciones que lo reciban.



Fragmentación: el objetivo es aumentar la fiabilidad al evitar retransmisiones en canales con altas tasas de error. Las tramas MAC se comparan con un umbral de fragmentación, de modo que, si el tamaño de la trama supera ese tamaño, se fragmenta. Todos los fragmentos son enviados secuencialmente. La estación mantiene el control del canal esperando solo un periodo SIFS después de recibir el ACK de la estación destino. Cada fragmento enviado reserva el medio físico para el envío del siguiente fragmento utilizando el campo duración de la cabecera de la trama MAC.



4. NIVELES DE TRANSPORTE Y APLICACIÓN

4.1 NIVEL DE TRANSPORTE

Es un **nivel extremo a extremo**. No hay **ninguna entidad intermedia de transporte o aplicación en ningún router**. Las interacciones en el nivel de transporte se basan en **comunicaciones directas entre dos procesos pares sin intervención de ninguna entidad intermedia**.

Control de errores:

- ❖ **Lógicos:** bytes perdidos, desordenados o duplicados asociados a los mensajes de aplicación (en el campo datos de los segmentos TCP).
- ❖ **Físicos:** bits cambiados en el segmento TCP. Encapsulado en el campo datos de un paquete IP. No los detecta IP porque solo los detecta en su cabecera.

Mecanismos del control de errores: todos los bytes de datos del mensaje de aplicación contenidos en el campo datos de cada segmento TCP dispone de:

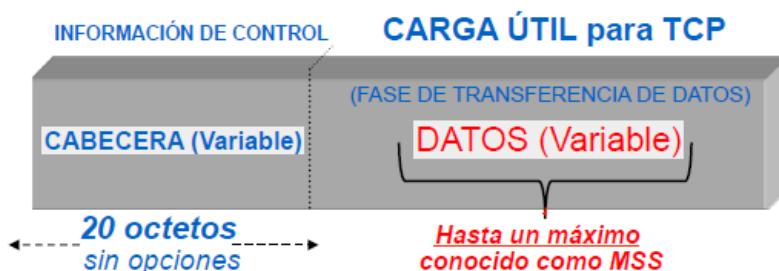
- ❖ **Número de secuencia:** cada byte tiene el **suyo propio**
- ❖ **Confirmación:** se confirma la **numeración de todos los bytes**. El **contenido de cada segmento tiene su propia confirmación**. Solo se confirma el contenido de un segmento TCP y no el propio segmento que no va numerado.
- ❖ **Temporizador o plazo de espera:** cada vez que se envía un segmento TCP se activa un **temporizador asociado al campo datos de dicho segmento**. Si no llega confirmación en el tiempo de espera prevista se **retransmiten los bytes de datos del segmento**.

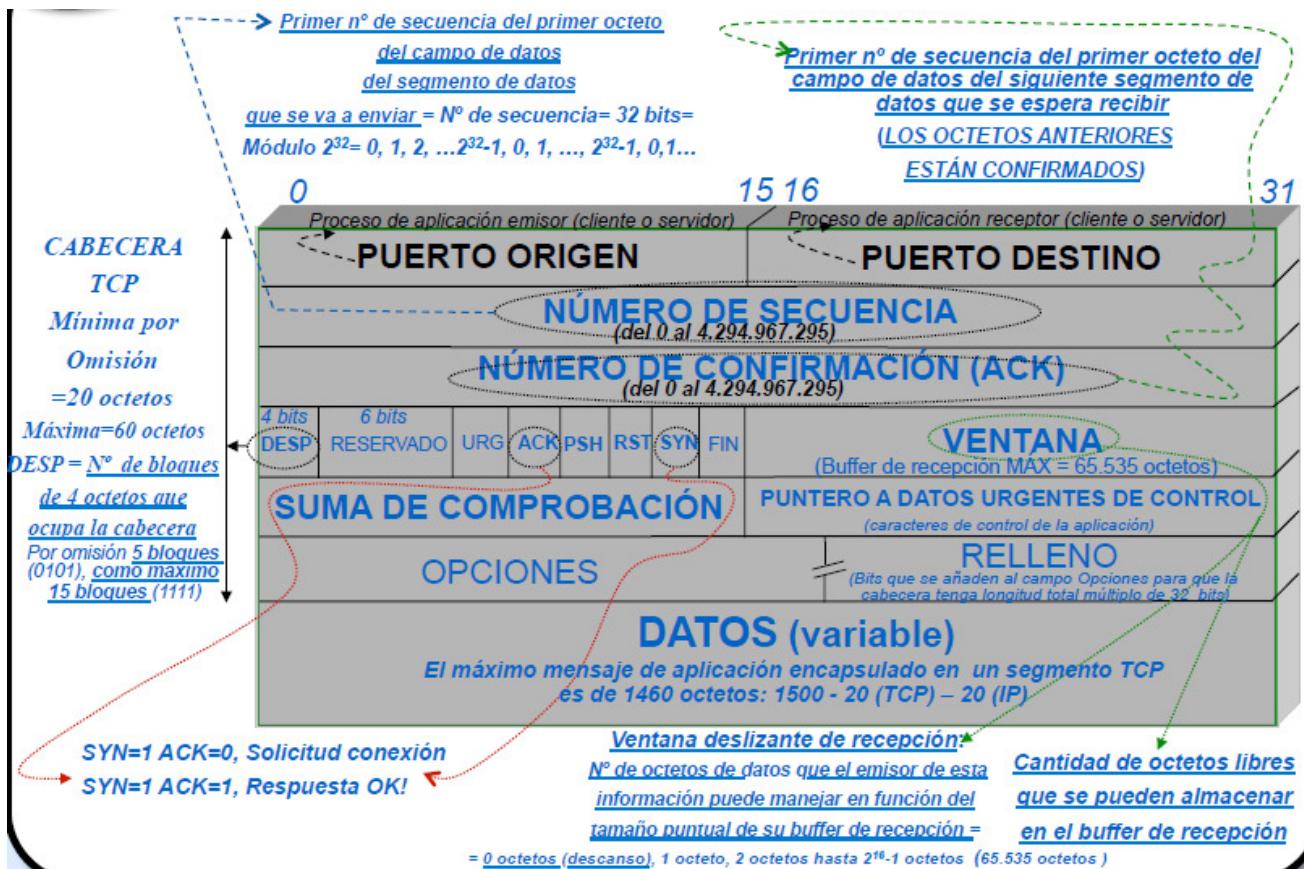
Diseño operacional TCP: todo proceso o protocolo de aplicación montado sobre TCP se **despreocupa de delimitar sus mensajes**. El proceso de aplicación va pasando a TCP sus mensajes de aplicación en flujos de octetos de una determinada longitud (byte-streams). Depende del tamaño del buffer de transmisión. A medida que se reciben esos bytes la entidad TCP los va almacenando, numerando y agrupando en segmentos TCP de datos para su envío a IP. Por esta razón TCP no numera los segmentos TCP de datos transmitidos sino los bytes contenidos en el campo datos de dichos segmentos.

Control de flujo: evitar que una entidad o proceso TCP transmita segmentos TCP más rápido de lo que otra es capaz de almacenar y procesar. Lo ejerce la entidad TCP receptora, que indicará al emisor el tamaño de su ventana de recepción para que ajuste adecuadamente su ventana de emisión. A medida que el buffer de recepción se va llenando la ventana de recepción se reduce si no se pueden pasar esos bytes al proceso de aplicación porque aún no han llegado bytes anteriores. Tanto cuando se va llenando como cuando finalmente se libera la entidad receptora se lo comunica a la emisora. La confirmación de que un byte se ha recibido se hace enviando el número de secuencia que se espera a continuación. Si se envía un número que no está en la ventana de emisión, se desactivan los temporizadores y se desliza la ventana de emisión para enviar el siguiente grupo de bytes.

Multiplexado TCP: a través de los números de puerto podemos tener muchos procesos TCP sin que se mezclen entre sí (HTTP, FTP, SMTP, etc.).

Segmento TCP: el tamaño máximo de los datos es el MSS (maximum segment size) que lo determina el receptor. Por omisión son 1024B de datos y 20B de cabecera.





Bit PuSH (PSH): mecanismo de empuje solicitado por la entidad de aplicación para que TCP proporcione un servicio forzado de transferencia. Lo activa la entidad TCP emisora cuando se lo indica su proceso de aplicación para forzar envíos y respuestas rápidos:

- ❖ **Envíos rápidos:** cuando la entidad de aplicación emisora desea evitar que su entidad TCP esté esperando más bytes de datos del propio proceso de aplicación para construir un segmento mayor o que la entidad TCP receptora pase los datos inmediatamente al proceso de aplicación sin almacenarlos previamente en el buffer de recepción.
- ❖ **Respuestas rápidas:** cuando la entidad de aplicación desea una respuesta inmediata de su entidad par de aplicación en el otro extremo.

Temporizadores de espera de confirmación: su valor se establece dinámicamente mediante algoritmos autoadaptativos que ajustan sus valores a la dispersión geográfica y el estado de la red según lo percibe la entidad de transporte emisora. El algoritmo Karn toma una muestra de RTT de cada segmento y su confirmación, hace la media y añade un margen de seguridad.

Opciones TCP: se especifican en la fase de establecimiento de conexión, en los segmentos de control con SYN=1.

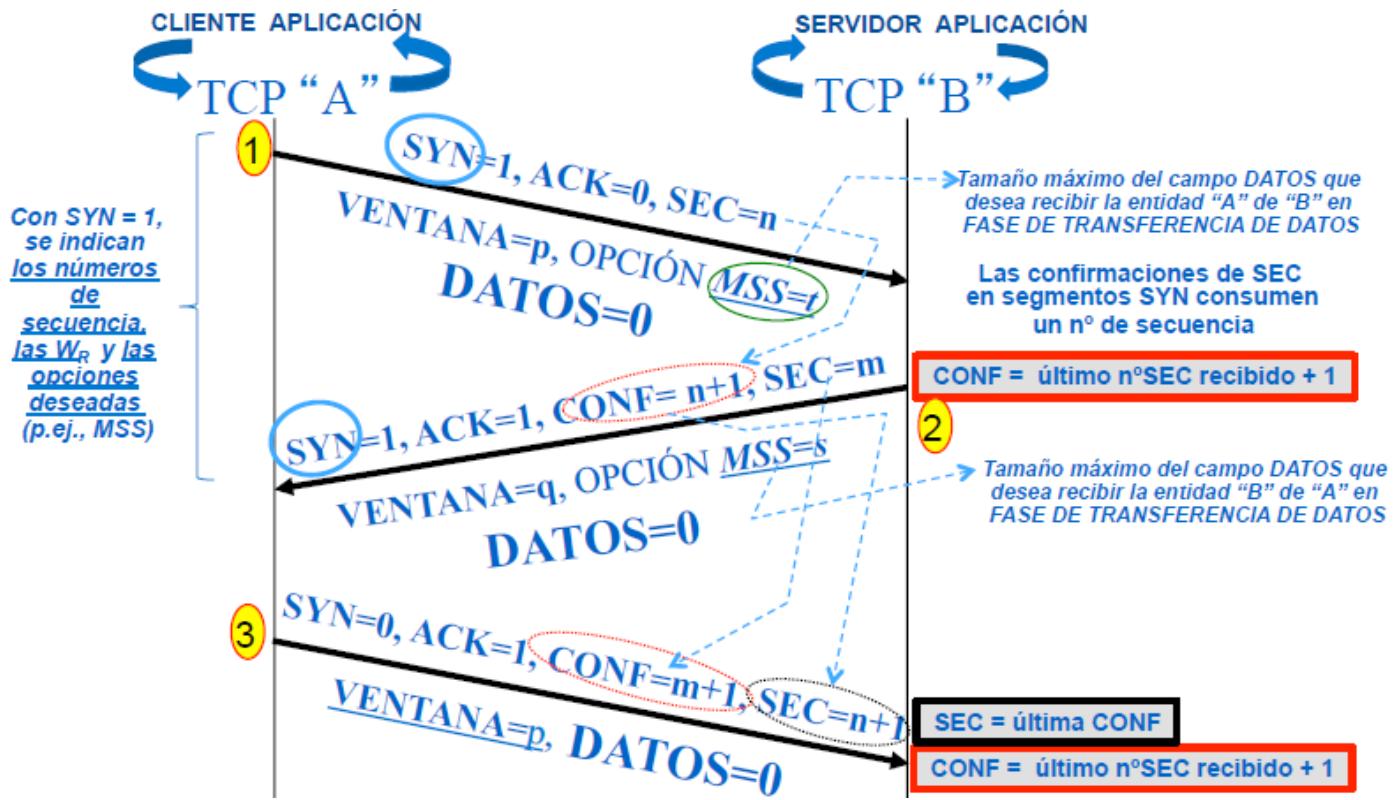


- ❖ **MSS:** cuando se desea un MSS diferente al de por omisión (1024B).
- ❖ **Factor de escala de ventana:** permite ampliar el campo ventana de 16 bits hasta un máximo de 30 bits.
- ❖ **Marca de tiempo:** permite al emisor configurar sus temporizadores de espera de confirmación.

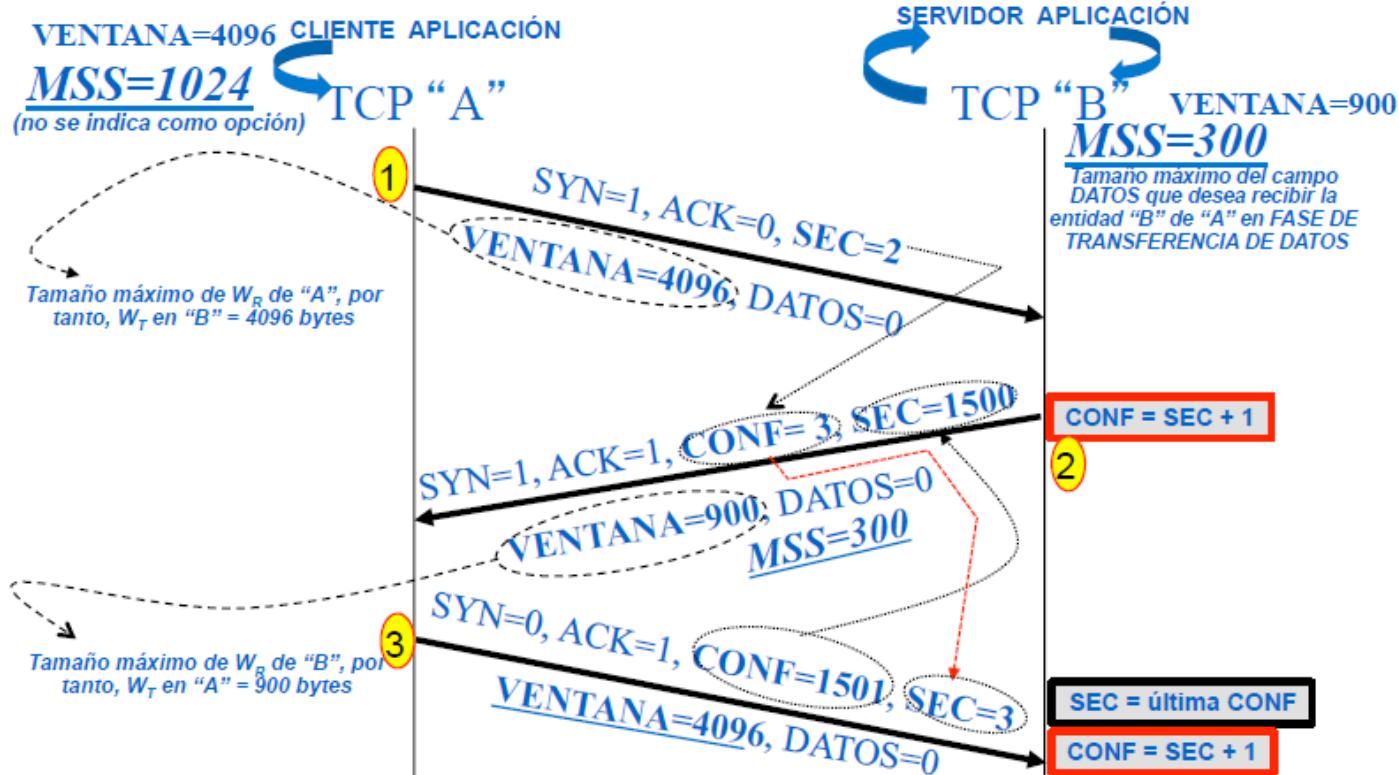
2	4	Valor MSS	MSS
3	3	Tamaño de la Ventana	Escala de la Ventana
8	10	Valor actual reloj emisor (4 octetos) + Respuesta Eco (4 octetos)	Marca de Tiempo

Fases de conexión: TCP es un servicio fiable con tres fases: establecimiento de conexión, transferencia de datos y liberación de conexión.

- ❖ **Establecimiento de conexión:** los números de secuencia iniciales se generan aleatoriamente y no se vuelven a usar en otras conexiones durante un tiempo prudencial para evitar confundir los números secuenciales de bytes de datos de segmentos de datos retrasados de una conexión anterior con los de las siguientes.



➤ Ejemplo:



❖ Transferencia de datos:

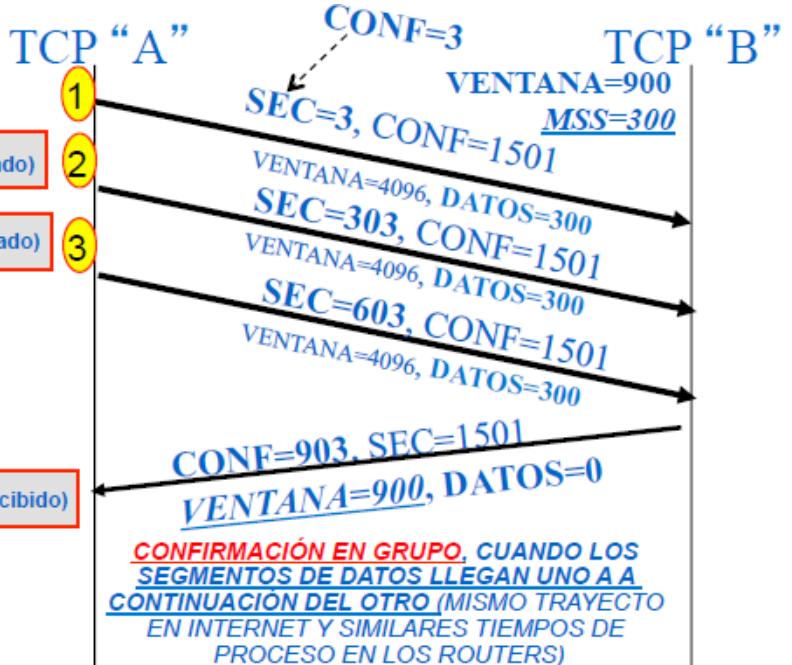
- Ejemplo de confirmaciones en grupo:

LOS SEGMENTOS LLEGAN SEGUIDOS UNO A CONTINUACIÓN DEL OTRO Y CORRECTAMENTE

SEC (enviado) = SEC+ DATOS (del último segmento enviado)

SEC (enviado) = SEC+ DATOS (del último segmento enviado)

CONF (enviada)= SEC+ DATOS (del último segmento recibido)



- Ejemplo de confirmaciones individuales:

LOS SEGMENTOS LLEGAN CORRECTAMENTE, PERO DE FORMA ESPORÁDICA

(DISTINTOS TRAYECTOS INTERNET y/o DISTINTOS TIEMPOS DE PROCESO EN LOS ROUTERS)

SEC (enviado) = SEC+ DATOS (del último segmento enviado)

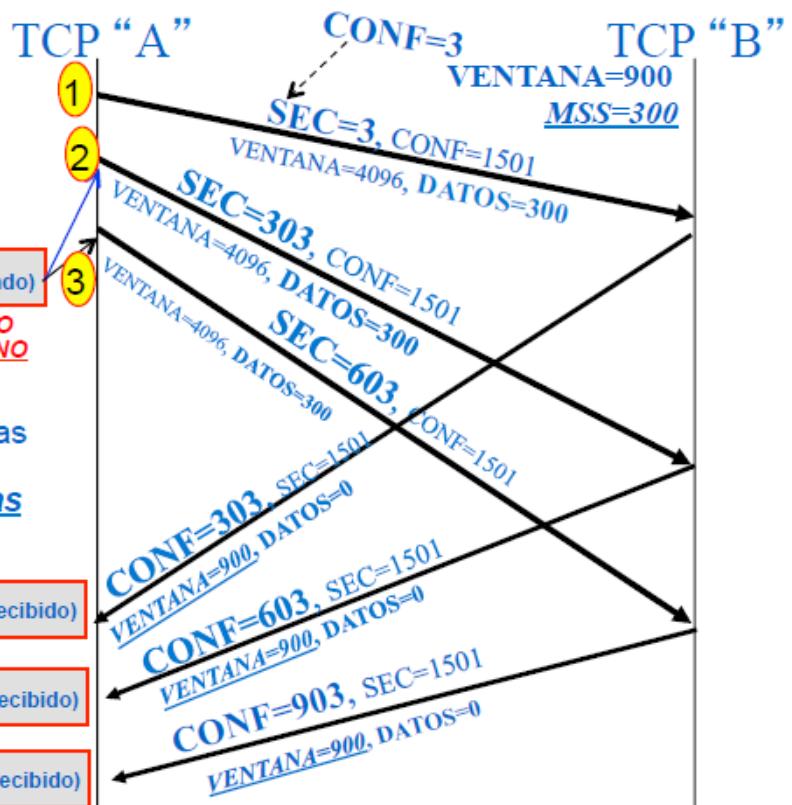
CONFIRMACIONES INDIVIDUALES, CUANDO LOS SEGMENTOS DE DATOS NO LLEGAN UNO A A CONTINUACIÓN DEL OTRO

A medida que van llegando las nuevas CONFs, se desactivan temporizadores, se eliminan copias y se desliza WT

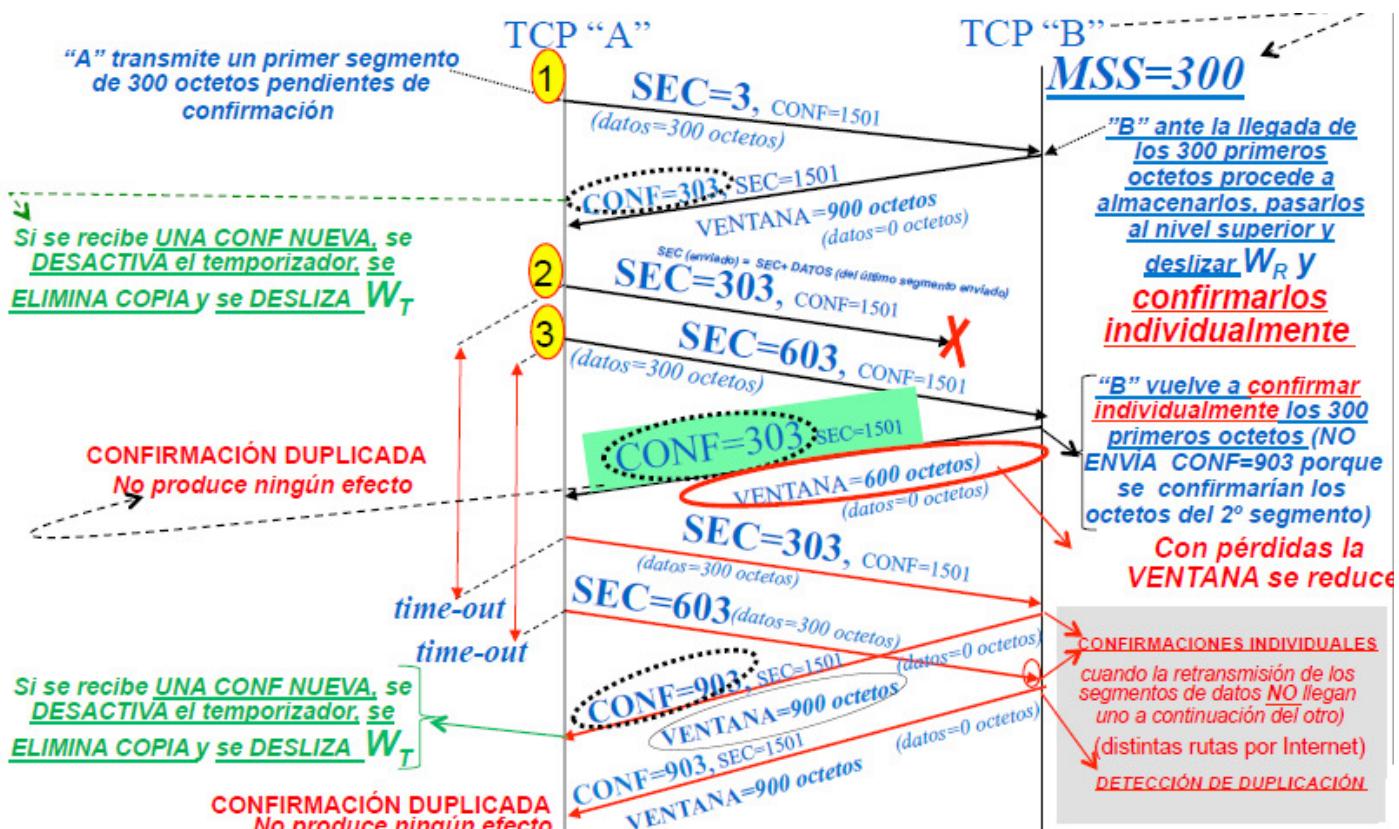
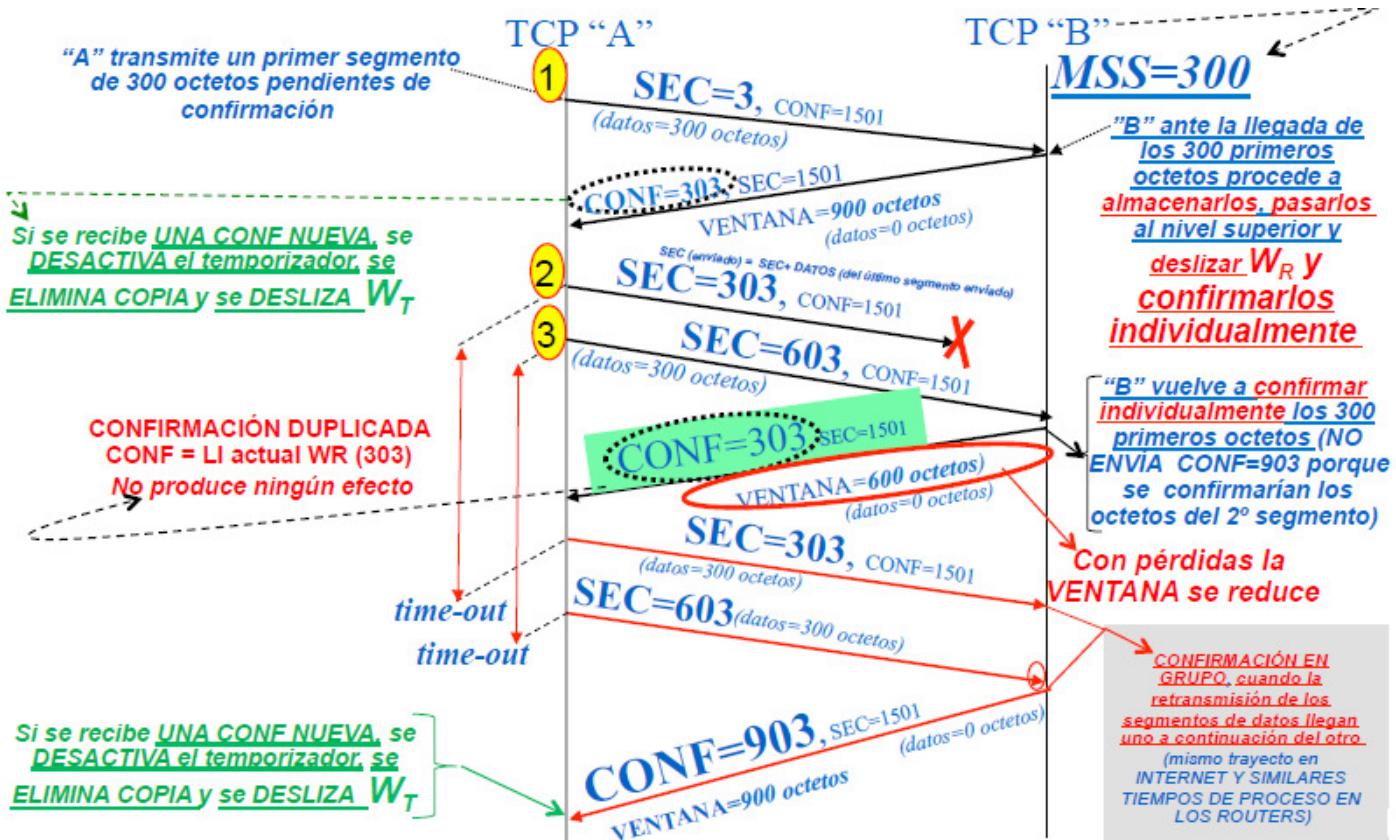
CONF (enviada)= SEC+ DATOS (del último segmento recibido)

CONF (enviada)= SEC+ DATOS (del último segmento recibido)

CONF (enviada)= SEC+ DATOS (del último segmento recibido)

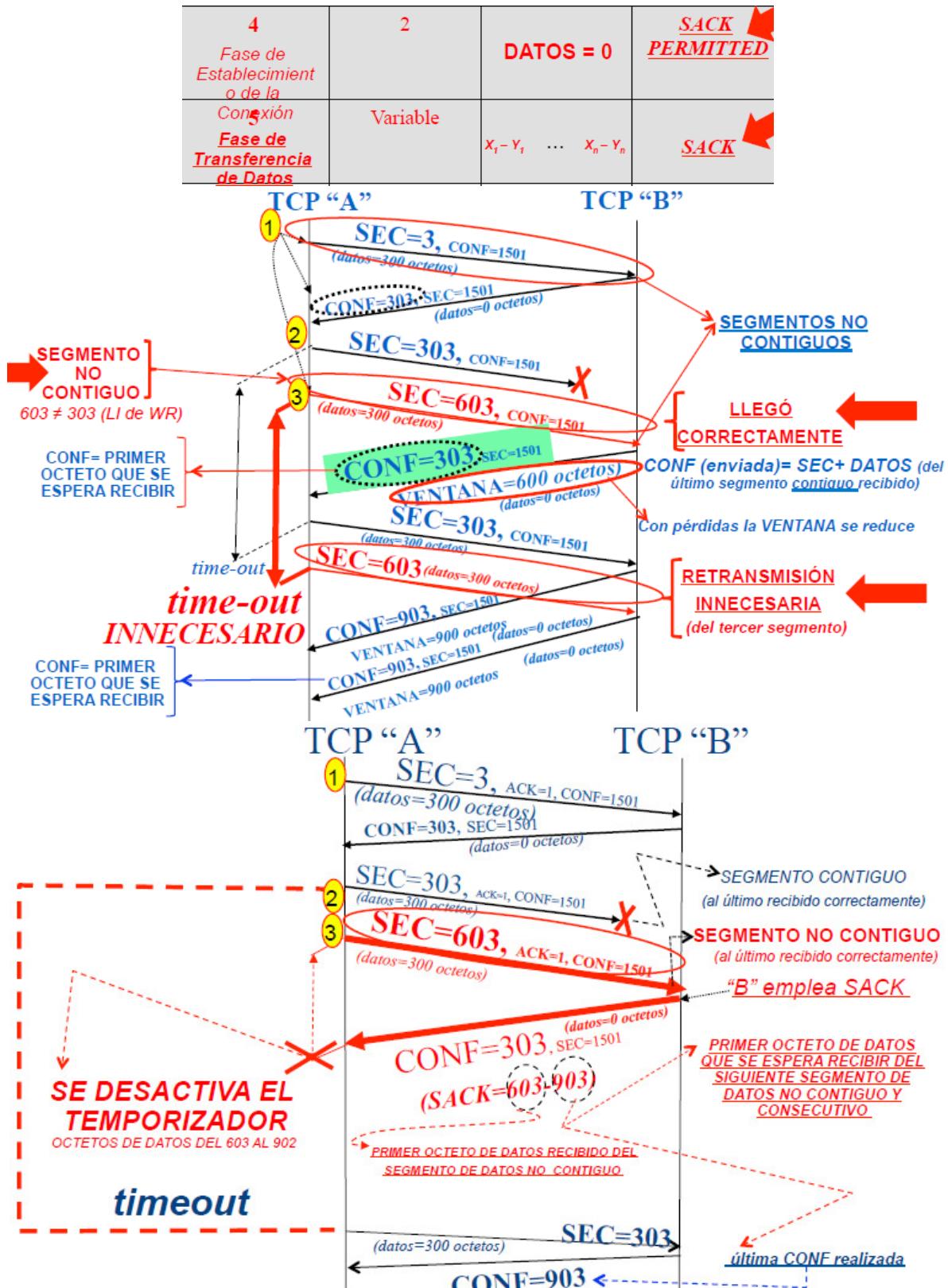


- **Ejemplo de transferencia con pérdidas:** lo principal a tener claro de las siguientes imágenes (con confirmación en grupo e individual) es que si algo se pierde se reenvía.



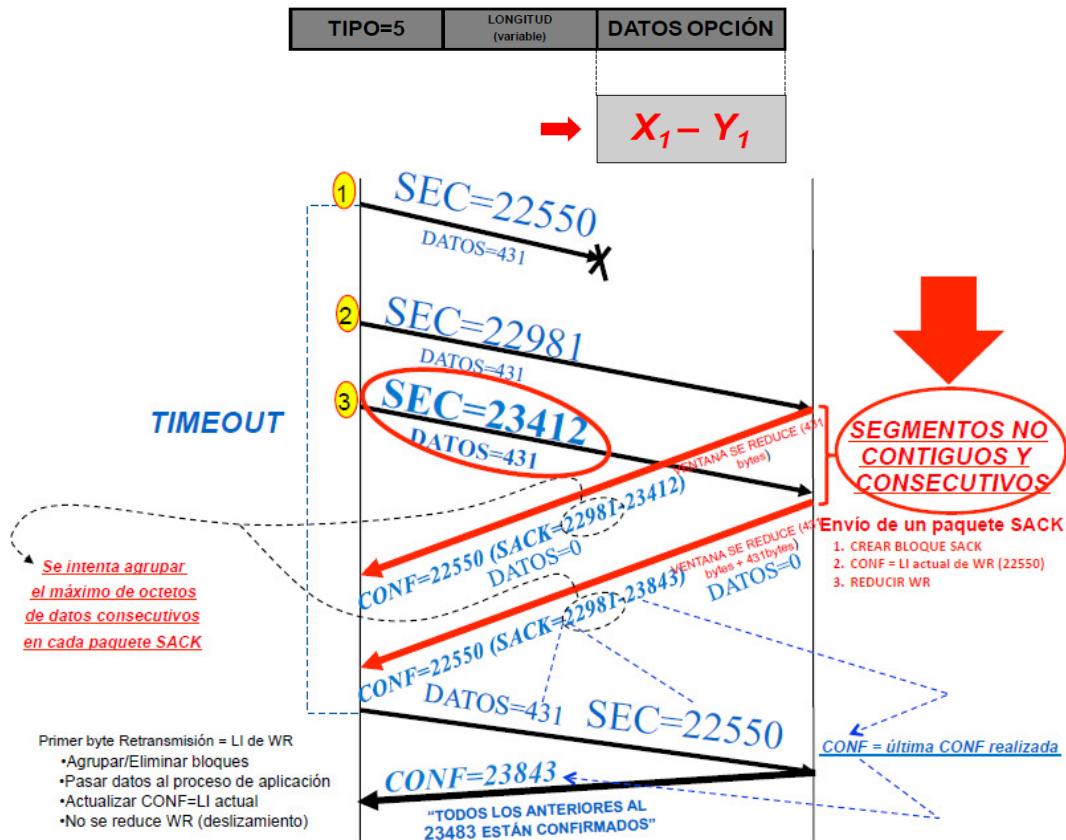
Opciones TCP (continuación):

- ❖ **Selective acknowledgement (SACK):** para hacer uso de SACK debe indicarse en la fase de establecimiento de conexión con la opción tipo 4. Si el receptor no ha recibido la opción tipo 4 no debe usar la tipo 5. Permite informar a la entidad TCP emisora de aquellos bytes de datos de segmentos de datos no contiguos que han sido recibidos correctamente. Un segmento no contiguo es aquel cuyo número de secuencia de su primer byte de datos no es el primero que se espera recibir. Evita vencimientos de temporizadores y retransmisiones innecesarias.

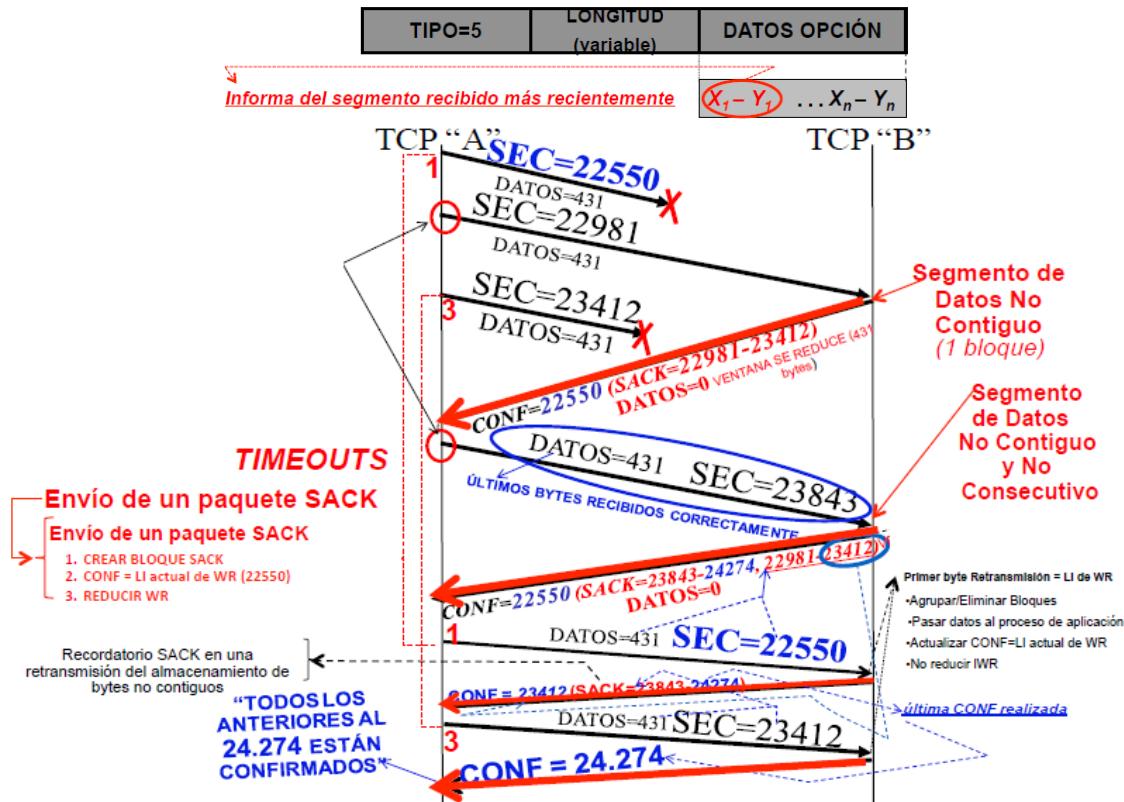


Hay dos tipos de SACK. Contigüidad se refiere a que son los siguientes que esperamos y consecutivos que no falta nada entre medias:

- Para segmentos de datos no contiguos y consecutivos (sin pérdidas): sea X_1 el primer byte de datos del primer bloque e Y_1 el último byte de datos del último bloque.



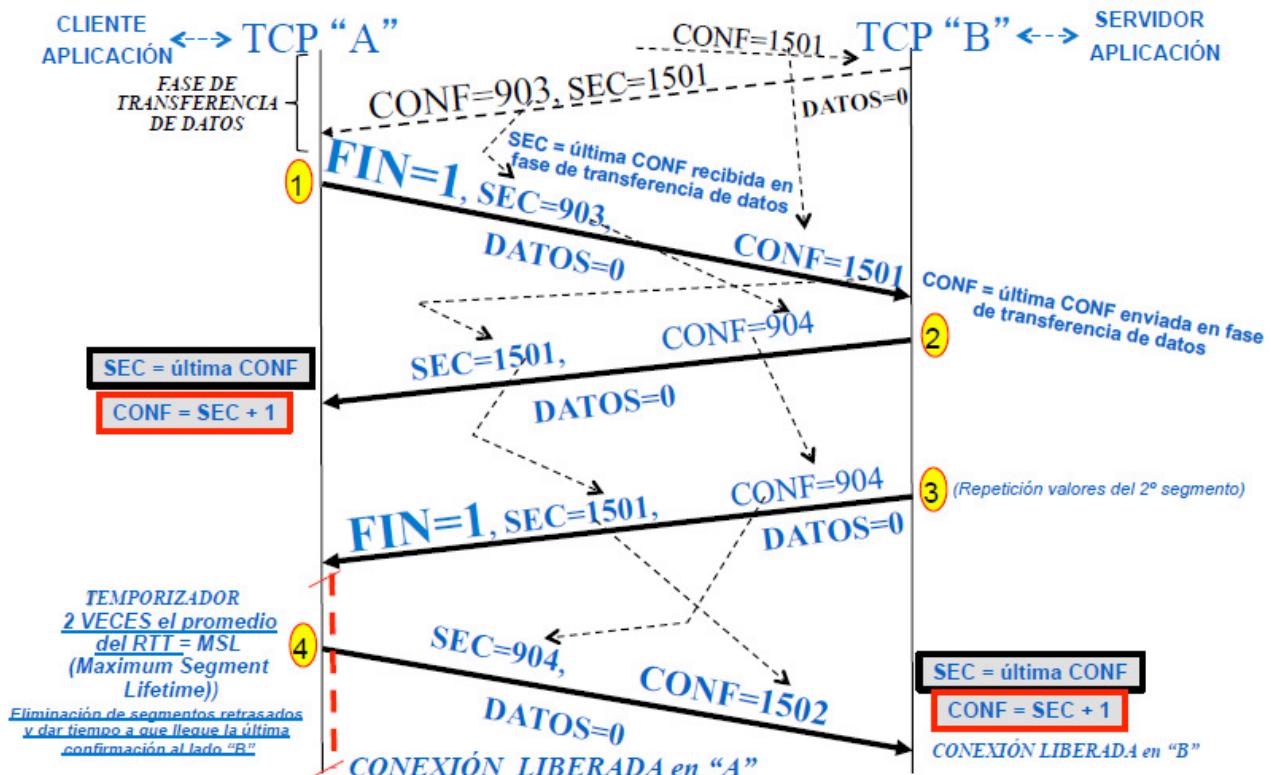
- Para segmentos de datos no contiguos y no consecutivos (con pérdidas): se pueden enviar hasta cuatro bloques no consecutivos. Despues del primer segmento los demás pueden estar listados en orden arbitrario.



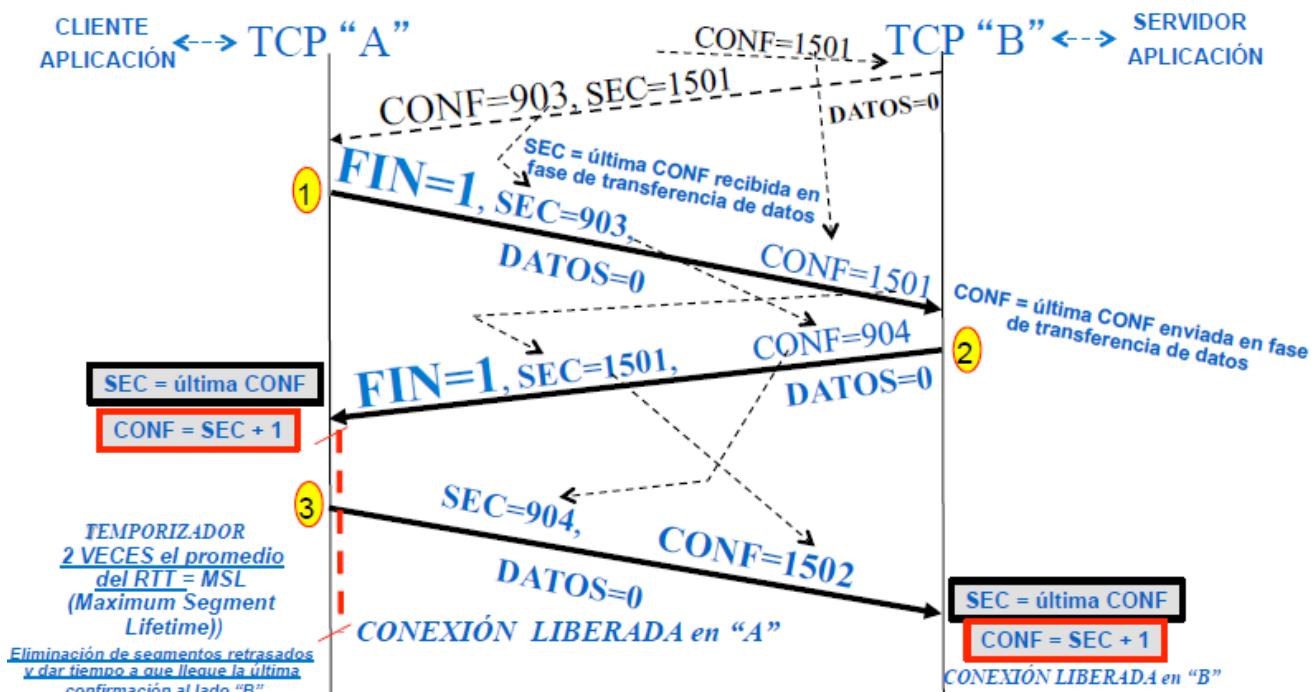
Fases de conexión (continuación):

❖ Liberación de la conexión:

- **Bilateral u ordenada:** bit FIN en los dos sentidos. La desconexión puede iniciarla cualquiera de los dos equipos invitando al otro a cerrar. El cierre de un sentido por parte de un equipo se interpreta como una invitación a cerrar al otro.
- **Basada en 4 envíos:** a FIN=1 se confirma con un segmento sin datos.



- **Basada en 3 envíos:** a FIN=1 se confirma con otro FIN=1.



- **Unilateral o abrupta:** bit RST sin datos en un sentido. Un equipo termina y cierra sin esperar a recibir confirmación. El otro se ve obligado a cerrar la conexión y eliminar los datos en buffers.

UDP: si la aplicación requiere un transporte rápido sin fiabilidad se monta sobre UDP, en vez de sobre TCP. Se utiliza en los siguientes escenarios:

- ❖ Aplicaciones en tiempo real: interactivas (videoconferencias) o no interactivas (streaming).
- ❖ Cuando el intercambio de mensajes es muy escaso y los mensajes son cortos, se producen regularmente y no importa si se pierde alguno.
- ❖ Envíos DHCP, consultas DNS, mensajes SNMP, mensajes NTP, etc.
- ❖ Cuando se envía tráfico de broadcast (establecer y liberar conexiones con los equipos vecinos).

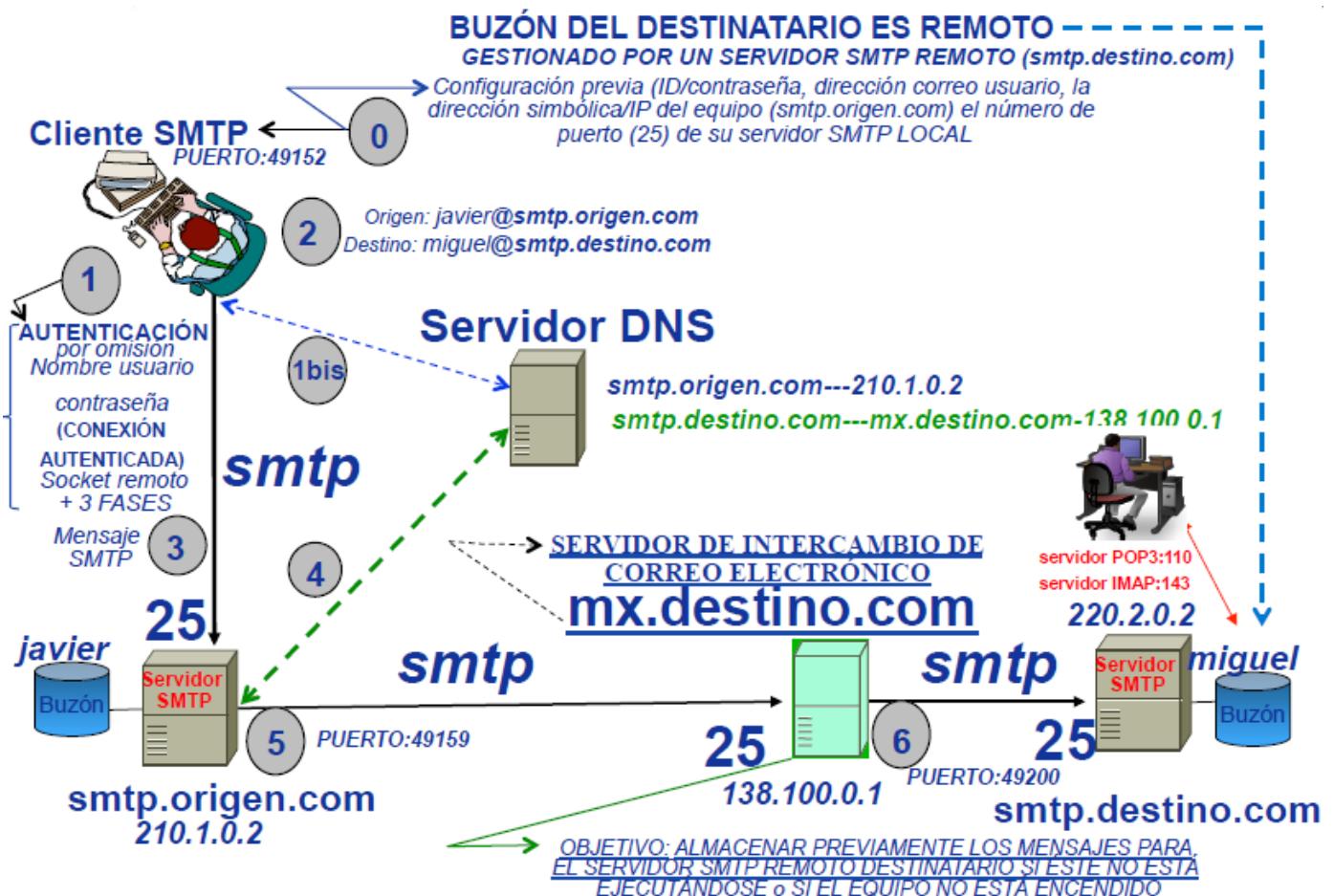
Al no ser fiable su única fase es la transferencia de datos. La detección de errores físicos es opcional (campo de suma de comprobación a 0) y no se recuperan. Los errores lógicos ni se detectan ni se recuperan. Es necesario por el multiplexado a través de los números de puerto.



4.2 NIVEL DE APLICACIÓN

Correo electrónico: tiene tres componentes principales;

- ❖ **Agente de usuario:** por ejemplo, Outlook
 - Entorno de correo en el equipo del usuario
 - Cliente de correo SMTP
 - Editor de texto
 - Codificador/Decodificador o códec MIME
 - Cliente de acceso al correo POP3/IMAP4 para recuperar el correo desde un buzón del destinatario en su servidor de correo a un directorio de su disco duro.
- ❖ **Servidor de correo SMTP del usuario:**
 - Se ejecuta en el equipo de la organización del usuario o en la red IP de su operador (ISP).
 - Buzones de los usuarios.
 - Colas de los buffers de los mensajes salientes.
- ❖ **Protocolo simple de transferencia de correo o protocolo de envío de correo SMTP:**
 - Enviar correo desde el cliente de correo SMTP de un agente de usuario a su servidor de correo SMTP.
 - Enviar correo desde el servidor origen o del remitente al servidor destino (buzón destinatario).



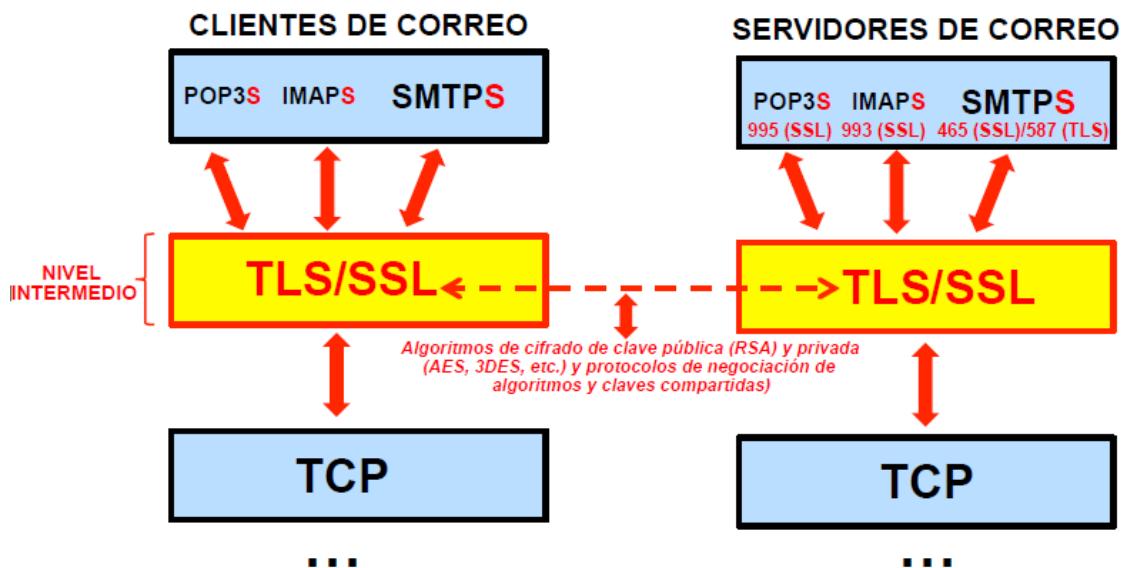
Para acceder al correo tenemos dos protocolos:

- ❖ **POP3:** proporciona un servicio de recogida de todos los mensajes. Casi no se utiliza ya que descarga los correos en la máquina del usuario y se borran del servidor. Para conectarse al servidor se usa el puerto 110.
- ❖ **IMAP4:** proporciona un servicio de gestión de mensajes en el mismo buzón de correo sin necesidad de descargarlos. Permite al usuario clasificar eliminar y distribuir su correo en distintas carpetas en el HDD del propio servidor de correo. También permite descargarlos al equipo del usuario si así se desea. Para conectarse al servidor se usa el puerto 143.

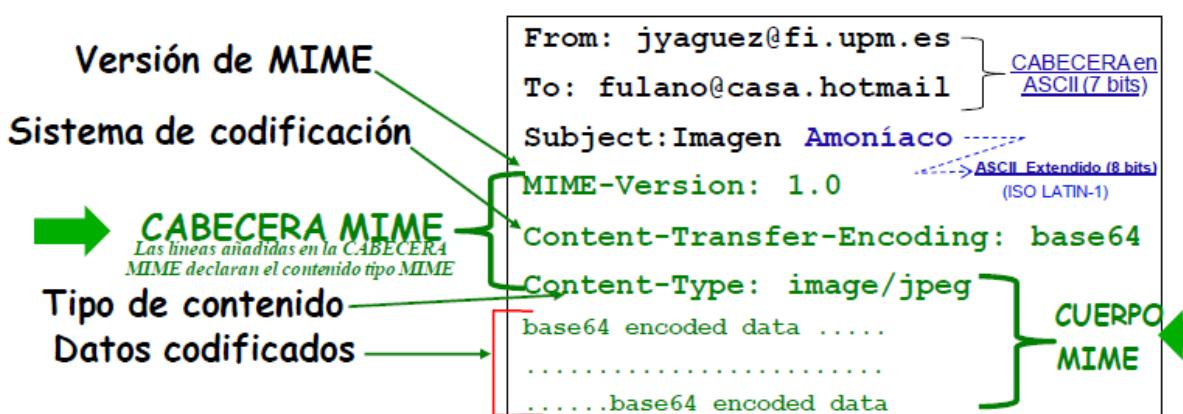
Puertos servidores SMTP:

- ❖ **25:** número de puerto para un servidor SMTP no seguro sobre TCP. El identificador de usuario y la contraseña son visibles. Reenvía cualquier mensaje transmitido por su cliente SMTP. Por tanto, hay peligro de que el cliente SMTP transmita voluntaria o involuntariamente por infección previa (spam o virus) y de que el servidor de correo origen entre en una lista negra de servidores SMTP y sus correos sean rechazados.
- ❖ **465:** número de puerto para un servidor SMTP seguro usado por la arquitectura de seguridad SSL (Secure Socket Layer) sobre TCP. El identificador de usuario y la contraseña se cifran, así como todo el correo enviado del cliente SMTP al servidor y viceversa. Permite el uso de firewalls para filtrar direcciones IP de clientes para el puerto 465. Permite el uso de filtros antispam, antivirus y listas negras de servidores SMTP.
- ❖ **587:** número de puerto para un servidor SMTP seguro basado en la arquitectura de seguridad TLS (Transport Layer Security) sobre TCP. TLS se basa en SSL y ambos son compatibles. TLS es más seguro, flexible y eficiente que SSL.
- ❖ **2525:** número de puerto opcional para un servidor SMTP seguro basado en la arquitectura de seguridad TLS sobre TCP.

Para poder cifrar y descifrar los mensajes de correo (y autenticación previa) entre el cliente y servidor SMTP, es necesario que tanto el cliente como el servidor SMTPTS dispongan de un Nivel Intermedio de Seguridad (TLS/SSL) entre TCP y el correspondiente proceso de aplicación SMTP. Ídem para los correspondientes clientes y servidores IMAP y POP3 para poder acceder al buzón y leer los correos de forma segura.

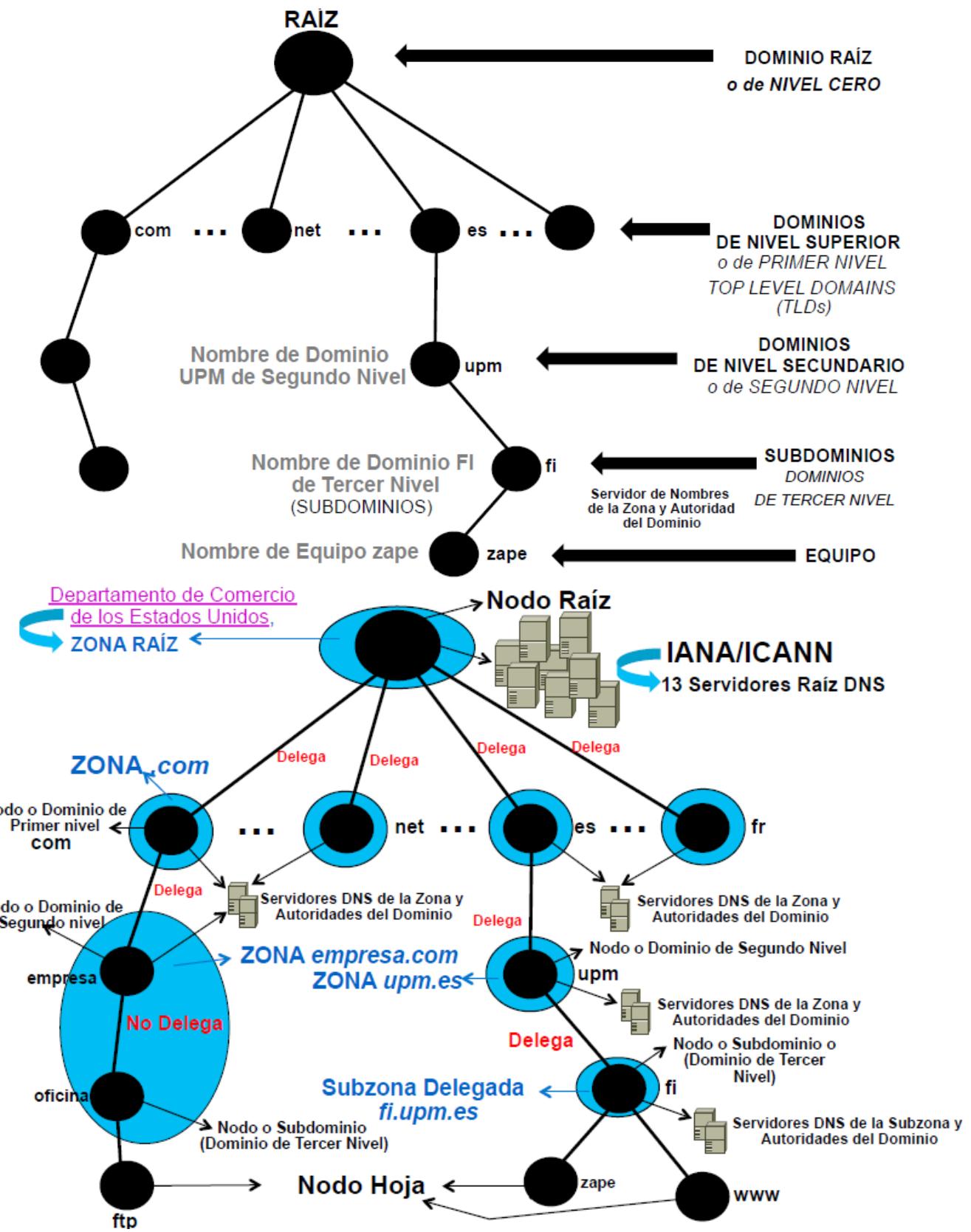


Los mensajes SMTP tienen una cabecera, seguida de una línea en blanco y los datos, que debe estar en formato ASCII de 7 bits. Para poder enviar mensajes no ASCII se emplea el codificador/decodificador MIME. Se agrega al campo datos una cabecera MIME y un campo datos MIME de forma individual tanto para el texto como para cada uno de los ficheros incluidos en dicho mensaje. A su vez el codificador MIME emplea un sistema de codificación para sustituir los datos STMP en grupos de 6 bits por un carácter en base64.

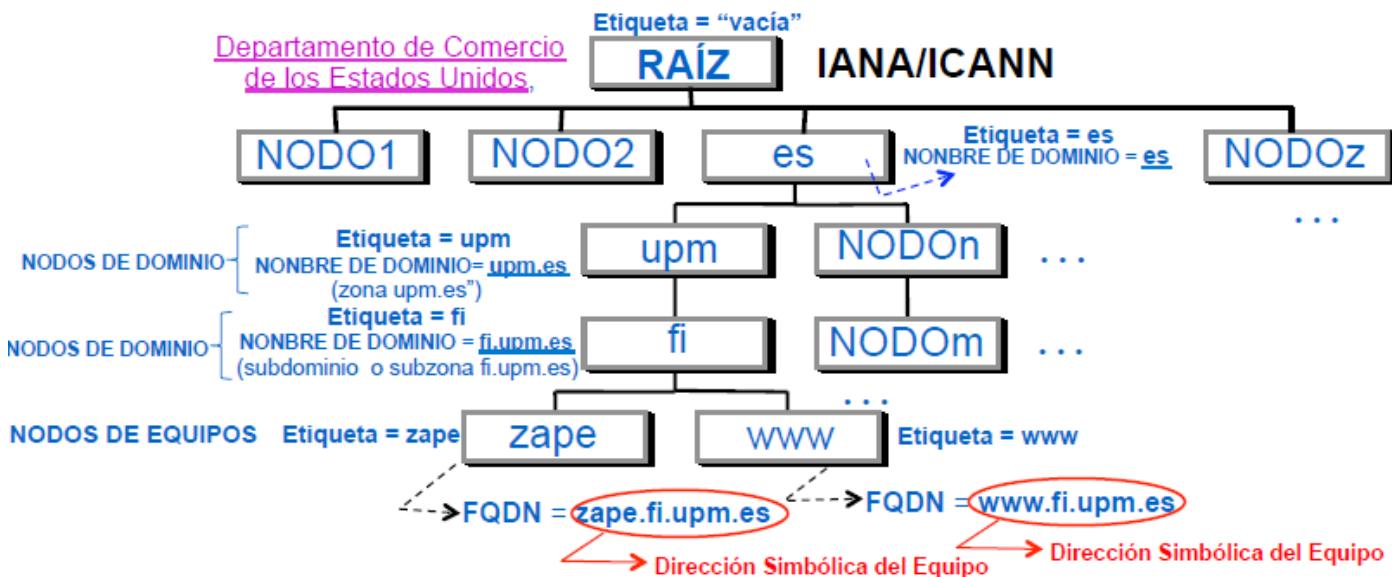


Sistema DNS: tenemos una base de datos distribuida en internet mediante servidores DNS locales de las diferentes organizaciones conectadas a internet. Mantienen registros locales con las asociaciones conocidas localmente entre los nombres simbólicos y las direcciones IP de la organización correspondiente. Ningún servidor DNS contiene la base de datos completa. El protocolo DNS pertenece al nivel de aplicación y sigue el modelo cliente servidor para la resolución de nombres simbólicos en direcciones IP.

La BD DNS en internet se representa mediante una estructura jerárquica de dominios DNS:

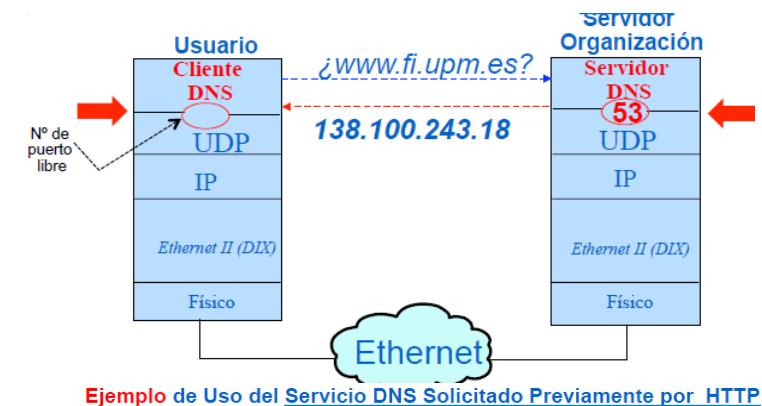


Cada nodo de dominio dispone de una etiqueta (nombre simbólico) y una dirección simbólica (secuencia de etiquetas separadas por puntos desde la etiqueta del propio nodo hacia arriba, es decir, hasta la raíz. Cada nodo de equipo dispone de una etiqueta y un FQDN (Fully Qualified Domain Name). FQDN o dirección simbólica del equipo es la secuencia de etiquetas separadas por puntos desde la etiqueta del propio nodo hasta la raíz. (por ejemplo www.fi.upm.es)



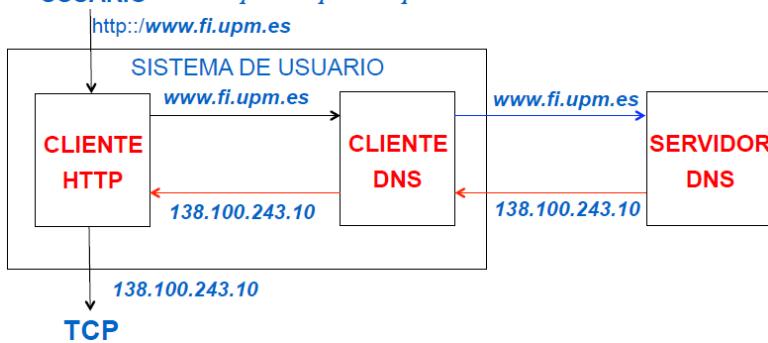
El dominio de gestión del primer nivel o top level domain (TLD) se corresponde con las etiquetas (nombres simbólicos) de primer nivel distribuidas en etiquetas genéricas (TLDs genéricos como .com, .org, .net) y etiquetas de países (TLDs países como .es, .uk, .fr)

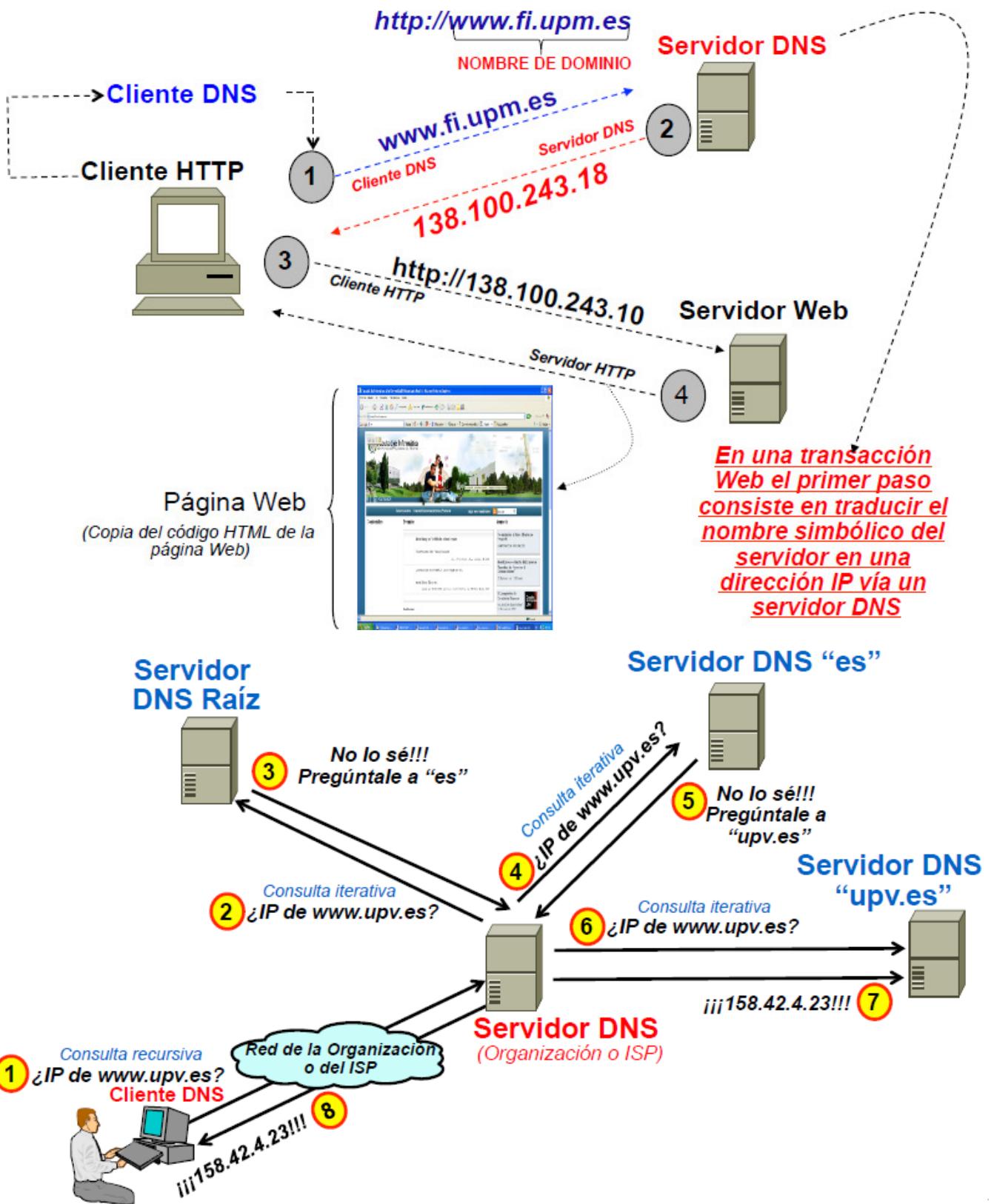
El protocolo DNS en el servidor usa el puerto 53 y en el usuario cualquier puerto libre. Da soporte a otros protocolos o aplicaciones como HTTP y SMTP. Un cliente DNS comienza resolviendo una dirección simbólica interrogando a su servidor DNS. Si un servidor DNS no tiene la resolución simbólica solicitada se convierte en un cliente de otro servidor DNS en la jerarquía DNS establecida en internet.



Ejemplo de Uso del Servicio DNS Solicitud Previamente por HTTP
Protocolo DNS da soporte a otros protocolos o aplicaciones como HTTP y SMTP entre otros

USUARIO *La resolución de nombres se hace de forma transparente por las aplicaciones del cliente*





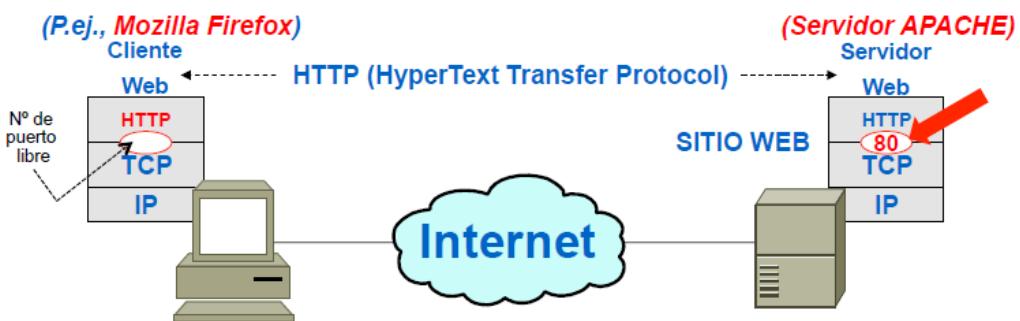
Para evitar un excesivo tráfico antes de lanzar el cliente DNS y dependiendo del SO hay unas interacciones previas para evitar mandar mensaje DNS por la red. Por ejemplo, el propio equipo de usuario va almacenando las traducciones DNS para no tener que solicitarlas al servidor (primero en /etc/host y luego en la memoria caché del navegador).

Una tabla DNS usa 5 atributos DNS fundamentales

- ❖ **Nombre de dominio:** identificador del recurso. Puede ser un nombre de equipo (FQDN es la clave principal de búsqueda) o un nombre de dominio.
- ❖ **TTL:** tiempo de vida del registro. Número de segundos que puede estar el registro en caché antes de ser descartado.
- ❖ **Clase:** Si el contenido es IN, identifica la clase del registro como clase INternet (o relacionada con los protocolos TCP/IP de Internet). Por ejemplo, para la clase IN existen tipos como: A, PTR, CNAME, MX, etc. CH (para un sistema no relacionado con Internet).
- ❖ **Tipo:** identifica el tipo de recurso descrito por el registro DNS.
 - **A:** registro que hace corresponder un FQDN y una IPv4.
 - **AAAA:** establece una correspondencia entre un FQDN y una IPv6
 - **PTR:** puntero a FQDN. Permite obtener un FQDN a partir de una dirección IP.
 - **CNAME:** permite resolver un alias. Por ejemplo, al introducir fi.upm.es (sin www).
 - **MX (Mail eXchange):** registro del servidor de intercambio de correo. Su objetivo es averiguar el servidor de intercambio de correo asociado al servidor SMTP remoto del usuario destinatario de correo. Pueden existir varios registros MX para la dirección simbólica del equipo servidor SMTP remoto, de forma que si el primero no está activo poder comunicarse con el siguiente.
 - **TXT:** plain text. Permite asociar información adicional a un dominio mediante múltiples cadenas de texto, con una longitud máxima de 255 caracteres cada una de ellas. Se usa, por ejemplo, para almacenar claves de cifrado.
- ❖ **Datos:** Es la información específica con el tipo de registro. Puede ser una dirección IP, un FQDN o una cadena ASCII.

NOMBRE DE DOMINIO	TTL	CLASE	TIPO	DATOS
www.fi.upm.es	84600 (24h)	IN	A	138.100.243.18
www.fi.upm.es	86400	IN	A	138.100.243.18
mail.fi.upm.es	86400	IN	A	138.100.243.11
zape.fi.upm.es	3600 (1h)	IN	A	138.100.8.1
18.243.100.138.in-addr.arpa	86400	IN	PTR	www.fi.upm.es
fi.upm.es (alias)	86400	IN	CNAME	www.fi.upm.es
www.fi.upm.es (FQDN)	86400	IN	A	138.100.243.10
smtp.destino.com	86400	IN	MX	mx.destino.com
mx.destino.com	86400	IN	A	220.2.0.2
mx.destino.com	86400	IN	TXT	"Servidor de Intercambio de Correo"

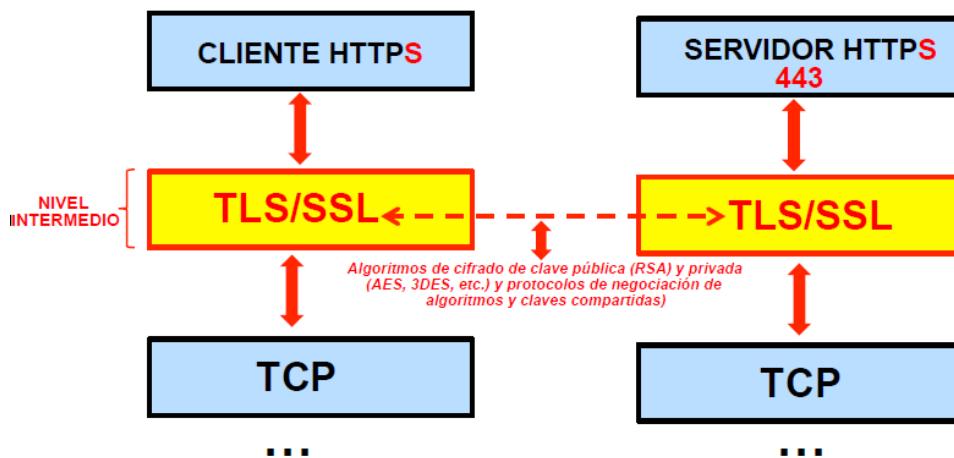
Protocolo HTTP: protocolo de presentación y distribución de cualquier tipo de información y acceso a cualquier tipo de servicio desde un cliente HTTP (navegador).



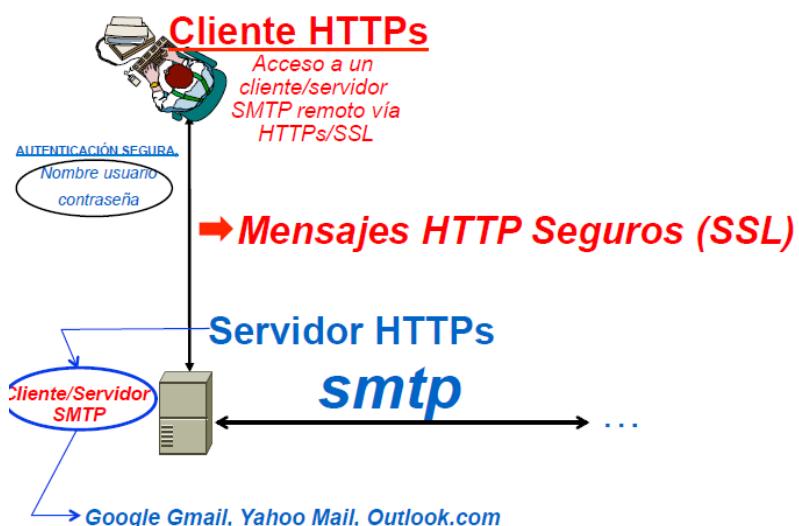
Hay dos tipos de servidores web:

- ❖ **Apache:** implementación libre de un servidor de código abierto multiplataforma para cualquier kernel. Configurable para distintas funcionalidades (por ejemplo, HTTPS). Por omisión su número de puerto es 80. Dicho puerto está reservado para el administrador de la máquina. Cualquier otro usuario con cuenta en dicha máquina que quiera disponer de su propio servidor web debe arrancarlo con número diferente.
- ❖ **Nginx:** implementación libre de un servidor de código abierto multiplataforma para cualquier kernel.

La descarga desde el cliente de los contenidos de un servidor web comienza por el fichero HTML de la página web inicial para su interpretación y visualización por un intérprete HTML en el navegador. Dicho fichero .html contiene enlaces locales o remotos a ficheros, de texto, audio, imagen, etc. y accesos a otros servicios como webmail, etc.



HTTP permite el acceso a webmail, lo cual es un acceso vía HTTP a un cliente/servidor SMTP en un servidor web remoto.

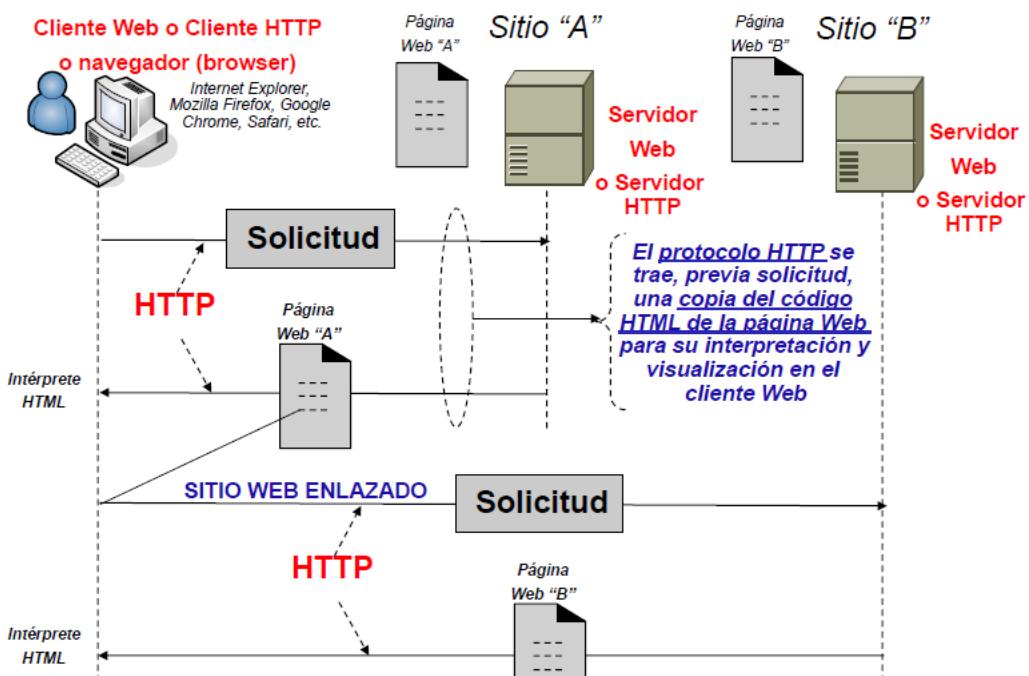


Para que el protocolo HTTP localice en internet un fichero mantenido por un servidor HTTP se utiliza una dirección HTTP en formato URL que consta de cuatro parámetros: protocolo://equipo:puerto/ruta.

- ❖ **Protocolo:** HTTP
- ❖ **Equipo:** alias o dirección simbólica del sitio Web (generalmente, comienza por www) o dirección IP. En una transacción Web el primer paso, generalmente, consiste en traducir el nombre simbólico del servidor en una dirección IP vía un servidor DNS.
- ❖ **Puerto:** Número entero que identifica al proceso servidor (campo opcional, si no aparece se asume que es el 80)
- ❖ **Ruta:** camino (path) de directorios (separados por "/") para acceder al Fichero y/o Fichero



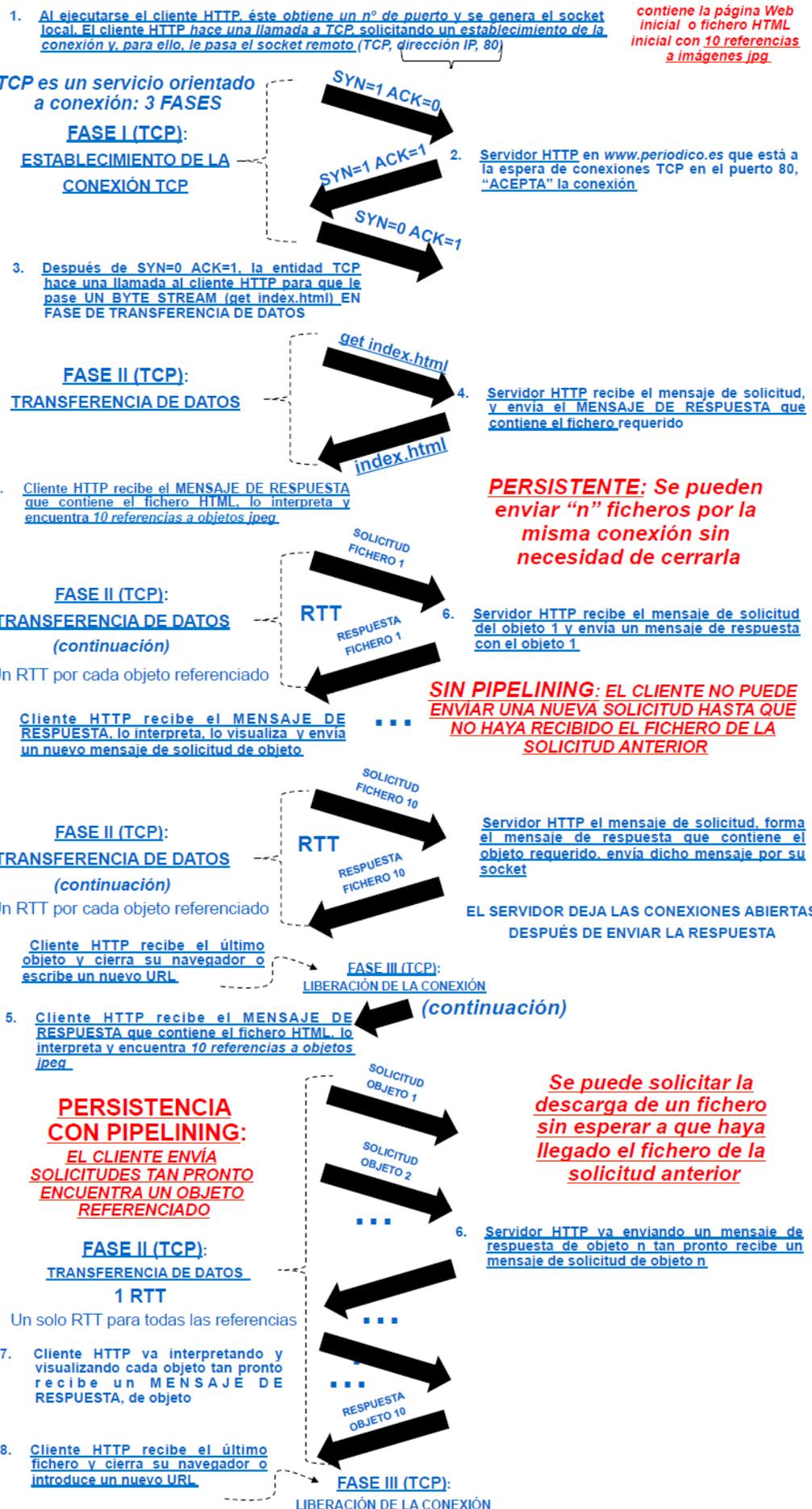
Ejemplo de descarga de la página web inicial:



HTTP 2.0 es la última versión de HTTP en internet. Funciona según el modelo cliente y servidor. Tiene las siguientes características:

- ❖ **Persistente:** la conexión TCP persiste independientemente del número de descargas de ficheros. Permite descargar dos o más ficheros en la misma conexión TCP.
- ❖ **Con pipelining:** por omisión. Permite enviar una nueva solicitud de fichero sin esperar a que llegue el fichero de la solicitud anterior, es decir, permite enviar tantas solicitudes como ficheros haya referenciados en el código HTML (sin esperar a los ficheros de invocaciones previas). Un solo RTT o tiempo de ida y vuelta común para todas las solicitudes y respuestas.
- ❖ **Sin pipelining:** el cliente envía una nueva solicitud solo cuando haya recibido el fichero de la anterior solicitud. Un RTT diferente para cada fichero solicitado.
- ❖ **Sin estado:** el servidor HTTP no mantiene el estado o la información de las solicitudes o acciones de un cliente HTTP en un servidor HTTP al cerrarse la conexión TCP. Para mantener el estado el programador de la aplicación web puede gestionar dicho estado por encima de HTTP vía cookies. Las cookies son ficheros de texto o fragmentos de información que contienen las acciones del usuario para cada servidor web visitado y que se almacena en el disco duro del cliente. Cuando un cliente HTTP solicita la descarga de una página web envía junto a la solicitud al servidor las cookies que tenga con ese servidor. Esta información permite diferenciar usuarios y actuar de forma diferente dependiendo del usuario.

Ejemplo de HTTP 2.0 persistente sin pipelining (1^a y 2^a imagen) y con pipelining (1^a y 3^a imagen):



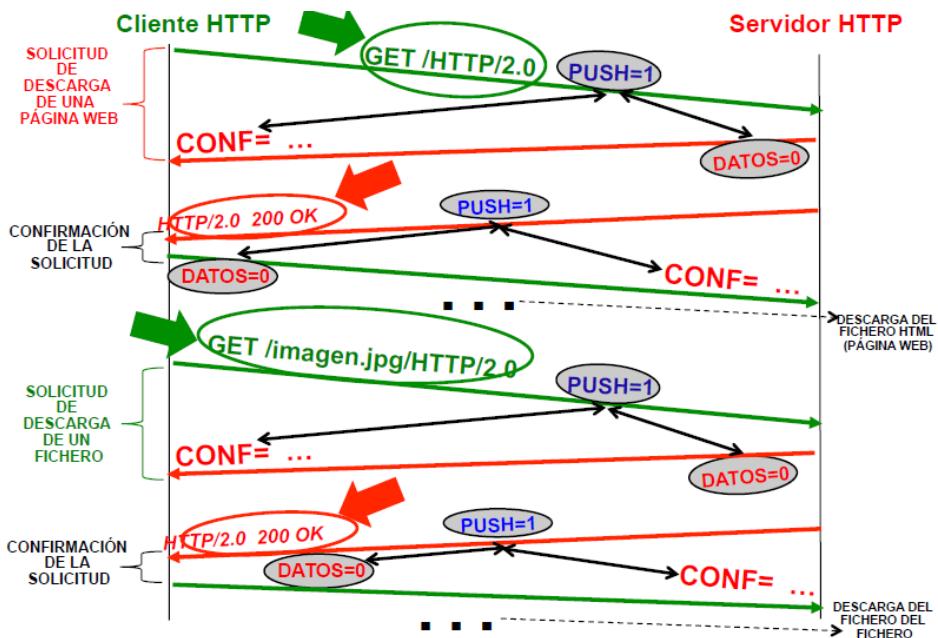
El formato de los mensajes HTTP consta de cabecera y campo de datos separados por una línea en blanco:



HTTP define 8 métodos implementados en el código del cliente HTTP que indican las acciones sobre el correspondiente recurso, de los cuales los 3 métodos o solicitudes más relevantes son:

- ❖ **GET:** Método HTTP asociado a un enlace en el código HTML de la página web descargada (aplicación) para solicitar un recurso (fichero, información, ...). La mayoría de las solicitudes HTTP son mediante GET. Se ejecuta, generalmente, cuando el usuario hace un clic en un enlace o, previamente, cuando el intérprete HTML encuentra una referencia, por ejemplo., un logo o imagen, mientras representa la página Web para el usuario.
 - Por ejemplo., obtención de un objeto llamado logo.png
 - GET /images/logo.png HTTP/2.0
 - A veces, GET incluye parámetros visibles que se encapsulan en la barra de direcciones en una búsqueda de información
 - Por ejemplo, /index.php?page=main&lang=es
- ❖ **POST:** Típico método HTTP utilizado en formularios para enviar parámetros o datos del usuario y que no son visibles en el localizador URL. El código del formulario exige que los datos introducidos se envíen vía post
- ❖ **PUT:** Método HTTP para enviar un fichero al servidor

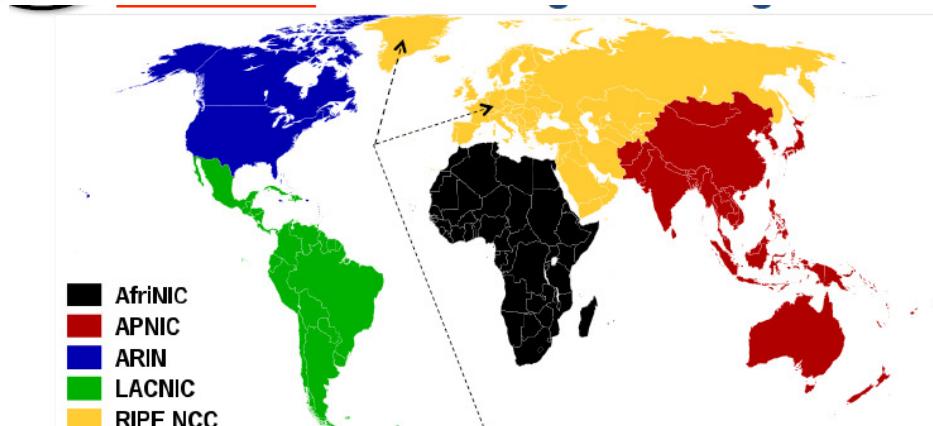
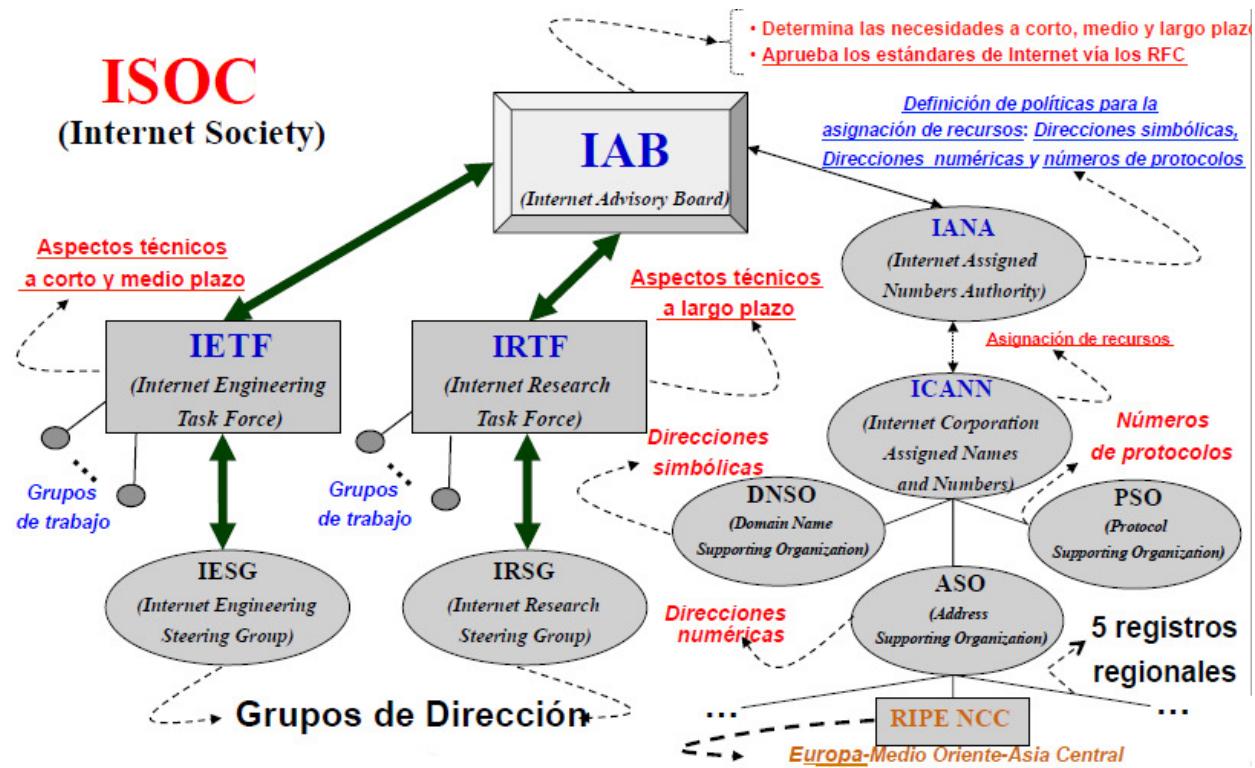
Los GETs (solicitudes) y las líneas de estado HTTP/2.0 200 OK (respuestas) llevan siempre el bit PUSH activado y PSH=1 requiere una confirmación sin datos.



5. REDES DE ÁREA EXTENSA E INTERNET

5.1 ORGANIZACIÓN Y FUNCIONAMIENTO DE INTERNET

- ❖ Organización de Centros de Control y Evolución Tecnológica en Internet: IAB,...
- ❖ Organización de Centros de Control de Acceso a Internet: ISPs (Internet Service Providers)
 - Niveles Jerárquicos
 - IXP (puntos neutros que interconectan los niveles con acuerdos de peering)
- ❖ Sistemas Autónomos y Encaminamiento Dinámico
 - IGPs y EGP (Interior/Exterior Gateway Protocol)



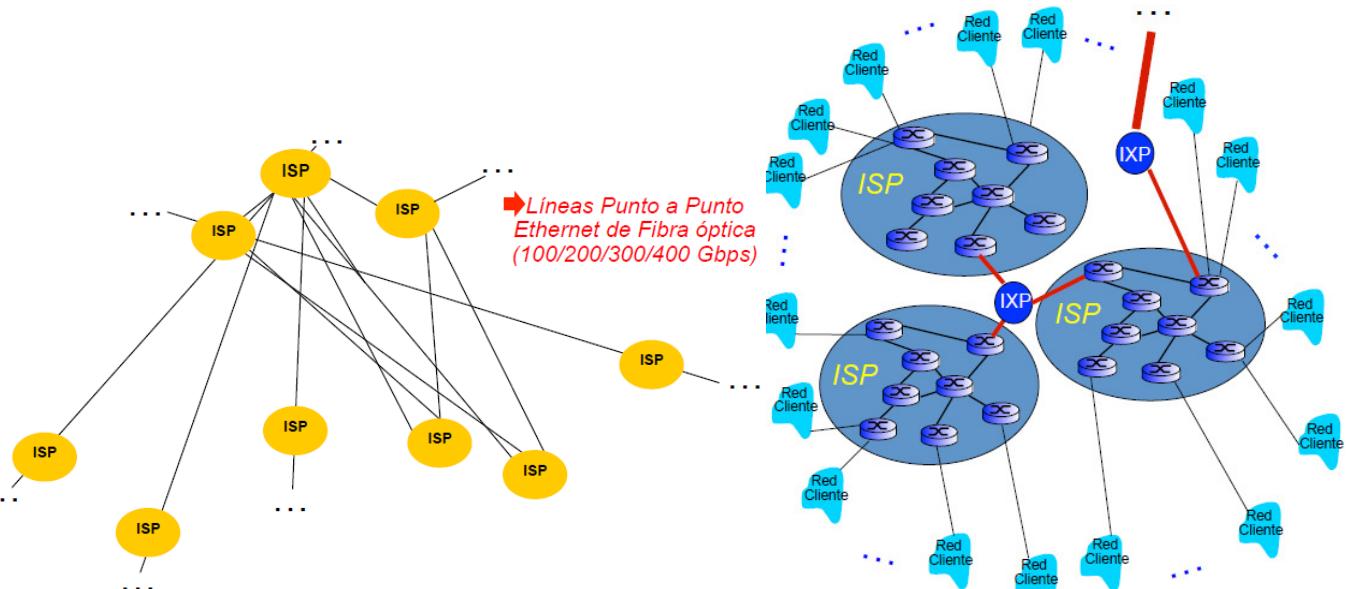
- American Registry for Internet Numbers (ARIN) para América Anglosajona
- RIPE (Redes IP Europeas) Network Coordination Centre (RIPE NCC) para Europa, el Oriente Medio y Asia Central: Amsterdam (Holanda) = www.ripe.net
- Asia-Pacific Network Information Centre (APNIC) para Asia y la Región Pacífica
- Latin American and Caribbean Internet Address Registry (LACNIC) para América Latina y el Caribe
- African Network Information Centre (AfriNIC) para África

Las especificaciones de protocolos, servicios y otras informaciones se recogen en unos documentos conocidos como RFCs que son documentos numerados en secuencia de forma cronológica por su número RFC.

Internet: internamente la red Internet está formada por la interconexión de las redes de routers de todos los operadores legalmente establecidos en cada uno de los países conectados a Internet. Las redes de los ISPs deben estar conectadas:

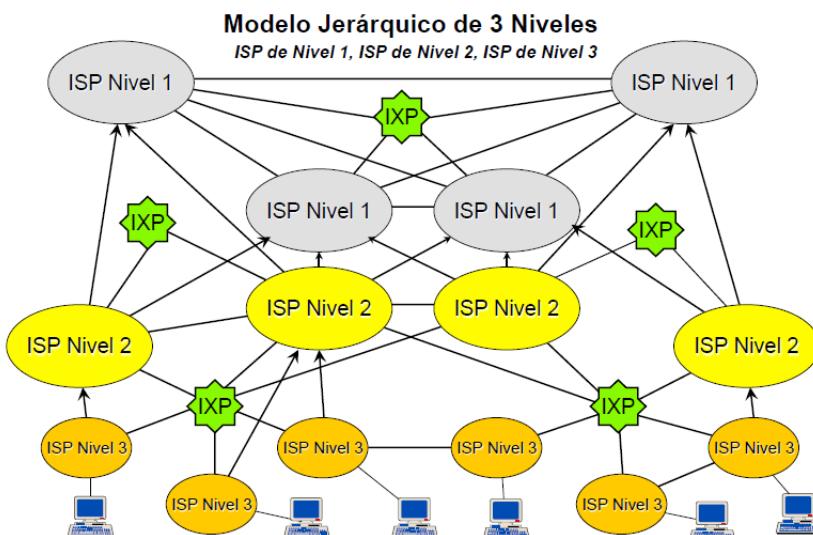
- ❖ **Directamente:** mediante enlace Ethernet punto a punto por fibra óptica.
- ❖ **Indirectamente:** mediante un centro de interconexión o punto neutro de intercambio (IXP). Los IXP son centros u organizaciones que ofrecen una infraestructura de comunicaciones (switches ethernet) para conectar las redes de routers de los ISPs.

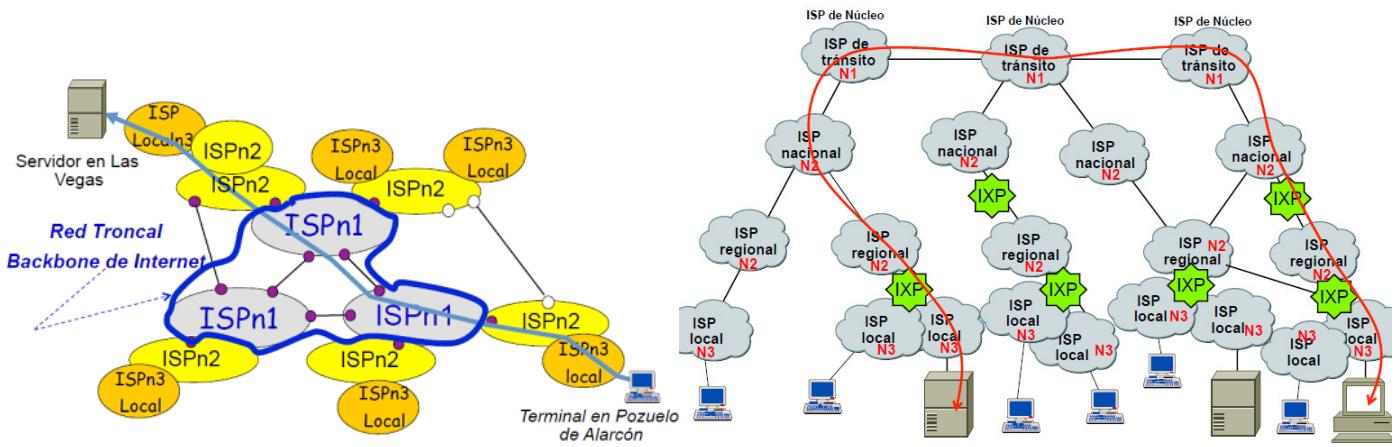
El objetivo es intercambiar previamente entre ISPs a través de un protocolo de encaminamiento dinámico la información de encaminamiento de rutas (Direcciones IP de los clientes de cada ISP). Así se pueden configurar automáticamente los routers y encaminar el tráfico de paquetes IP independientemente de que el destino pertenezca a un ISP u otro.



Aparte de estar conectados los ISPs (directa o indirectamente) es necesario que establezcan en primer lugar un acuerdo de peering (acuerdo entre pares). Generalmente, es el que realizan dos ISPs cuando acuerdan intercambiar rutas y tráfico sin cobrarse por el servicio que mutuamente se prestan. También el término suele aplicarse a cualquier acuerdo de intercambio de tráfico entre ISPs, incluso, cuando haya pago por el servicio. Esto ocurre, normalmente, cuando los dos ISPs son de tamaño muy diferente (el pequeño paga al grande).

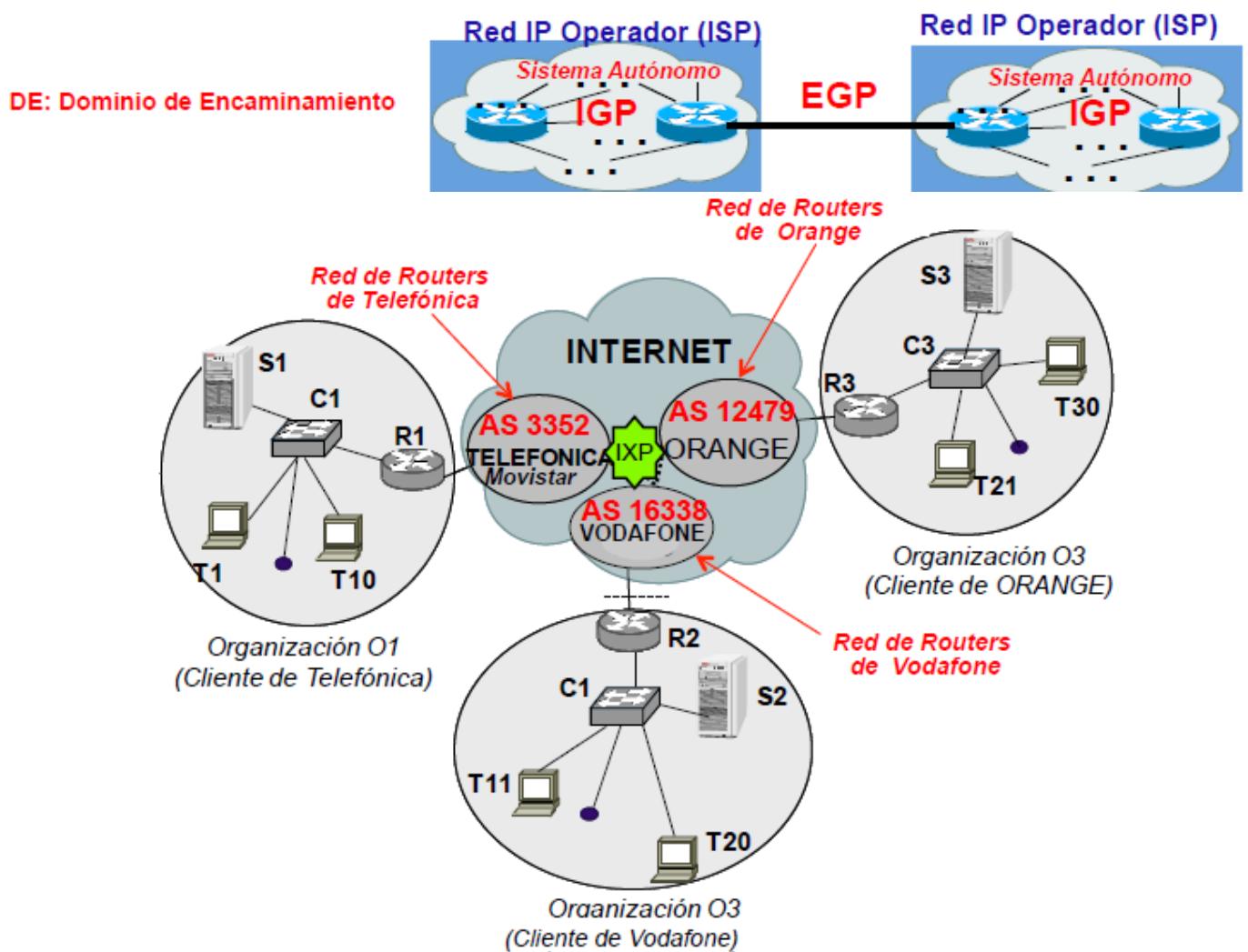
Los ISPs se clasifican en una jerarquía de tres niveles. El nivel 1 incluye una cobertura a nivel mundial o entre continentes. Los de nivel 2 cubren uno o varios países. Los de nivel 3 cubren a nivel regional o nacional.



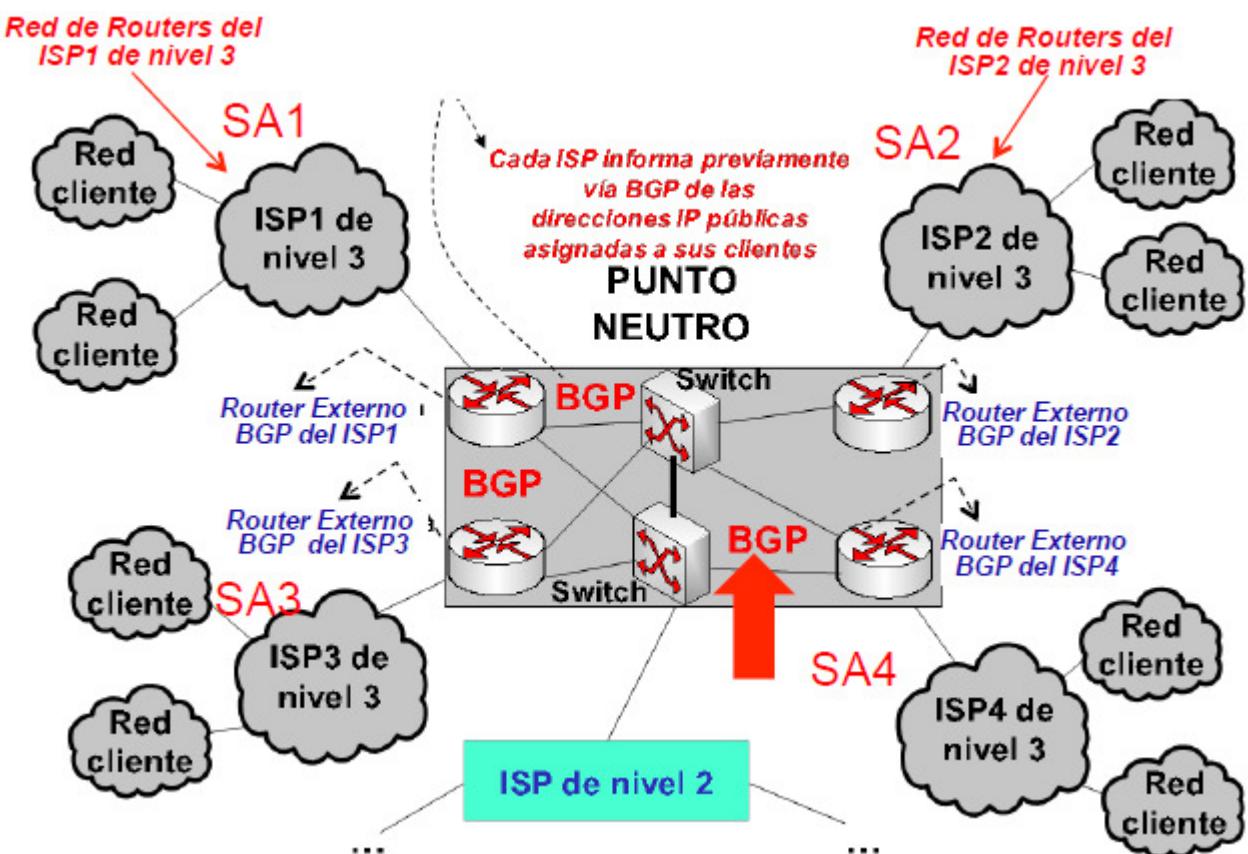


Los ISPs de nivel 3 pueden estar o no conectados a un ISP de nivel 2. Se interconectan entre si mediante los IXPs. Los ISPs de nivel 2 pueden ser clientes de uno o más ISPs de nivel 1. Los ISPs de nivel 1 forman el núcleo o backbone de internet.

Sistemas autónomos: conjunto de routers controlados por una única autoridad administrativa (administrador de la red IP del operador) que utilizan, en un mismo dominio de encaminamiento, un mismo protocolo interno (IGP: Interior Gateway Protocol) para la distribución y actualización de la información de encaminamiento internamente y que se conecta con otros sistemas autónomos de otros operadores mediante routers externos que utilizan un mismo protocolo externo (EGP: Exterior Gateway Protocol) para la distribución y actualización de la información de encaminamiento externamente entre sistemas autónomos. Todo sistema autónomo dispone de un número de identificación público de 16 bits.

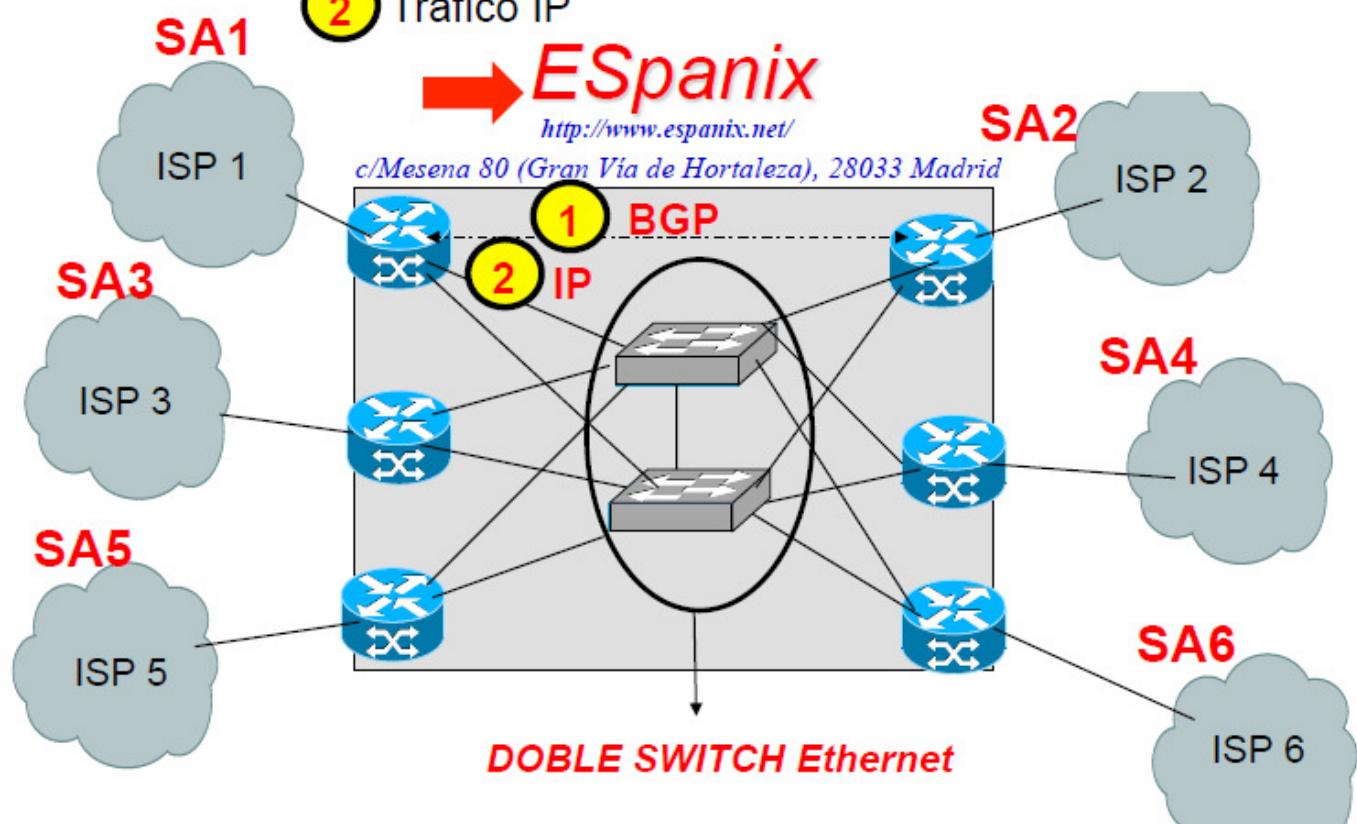


Implementación física de un IXP:



PUNTO NEUTRO EN ESPAÑA

- 1 Intercambio de Rutas (BGP)
- 2 Tráfico IP



Encaminamiento dinámico en Internet: se basa en configuración IP previa dinámica o automática. El objetivo es realizar la configuración sin parar ningún router de ningún sistema autónomo. Se utiliza un IGP de distribución y actualización de información de encaminamiento entre routers internos del sistema autónomo y un EGP de distribución y actualización de información de encaminamiento entre los routers externos de sistemas autónomos vecinos. Una vez configuradas las tablas IP se encamina el tráfico de la manera habitual mediante protocolo IP.

❖ Protocolos internos IGP (Interior Gateway Protocol)

- **RIPv2** (Routing Information Protocol): IAB
 - Protocolo estándar en Internet
- **IGRP** (Internet Gateway Routing Protocol): Cisco
 - Protocolo propietario de CISCO
 - RIP mejorado
- **EIGRP** (Enhanced IGRP): Cisco
 - Protocolo propietario de CISCO
 - IGRP mejorado
- **OSPFv2** (Open Shortest Path First Protocol): IAB
 - Protocolo estándar en Internet
- **IS-IS** (Intermediate System to Intermediate System): ISO
 - Protocolo estándar no específico en Internet (protocolo de la arquitectura de comunicaciones OSI adaptado a TCP/IP)

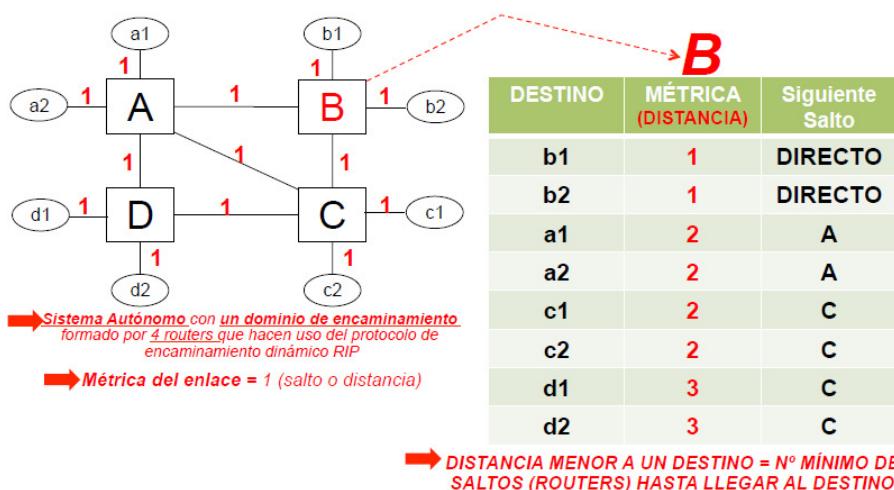
❖ Protocolos externos EGP (Exterior Gateway Protocol)

- **BGP-4** (Border Gateway Protocol 4): IAB entre Sistemas Autónomos
 - Protocolo estándar en Internet

Los protocolos de encaminamiento dinámico usan dos algoritmos:

❖ Vector de distancias o lista de distancias:

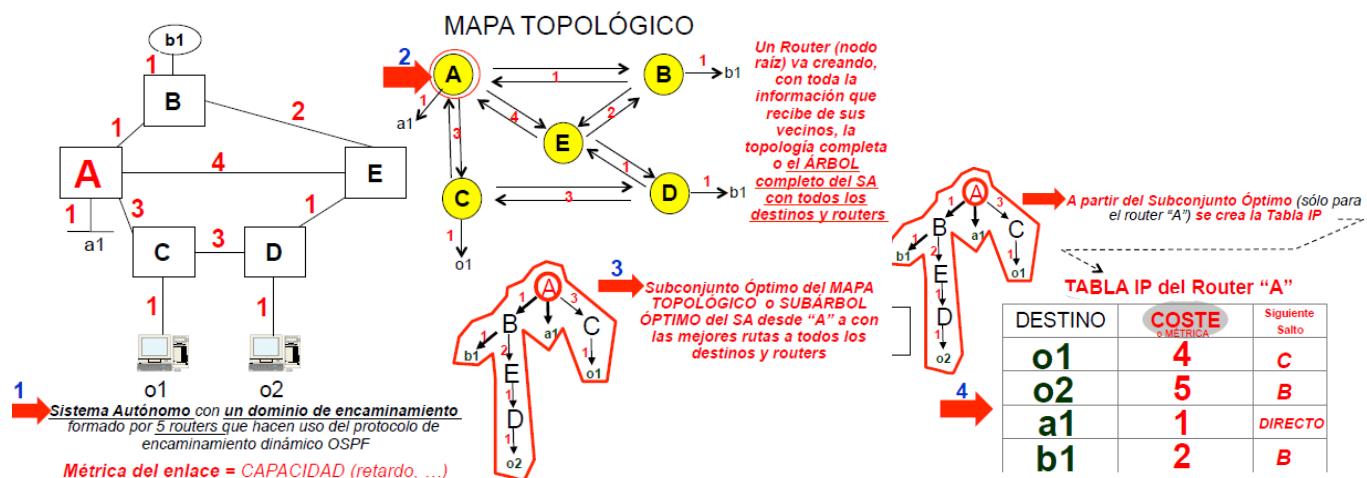
- **Métrica:** forma más básica y usada. La métrica es el número de routers que hay que atravesar hasta llegar a un destino, pero se pueden usar otras medidas como el ancho de banda, la capacidad del enlace, retardos, etc.
 - **Métrica del enlace:** asocia un mismo coste a un enlace.
 - **Métrica total a un destino:** suma menor de los costes de cada enlace hasta llegar al destino o número mínimo de saltos para llegar al destino.
- **Protocolo RIPv2:** métrica basada en el número de saltos (mínimo 1 máximo 15). Usa UDP y su puerto es el 520. Hace broadcast de tablas completas entre routers vecinos cada 30 segundos. Es seguro ya que todos los intercambios están previamente autenticados. Se usa en topologías simples con pocos routers y poco tráfico.



RIP tiene la limitación de que las rutas son fijas y pueden producir sobrecargas. Se desaprovechan caminos más lentos que sería eficiente tomar en caso de que haya mucho tráfico por el camino ideal.

❖ **Estado del enlace (Dijkstra) o algoritmo SPF (Shortest Path First) o el Primer Camino más Corto:** los protocolos son más complejos en su uso y configuración. Por el contrario, los mensajes intercambiados son generalmente cortos. Salvo en el inicio, cada router intercambia las actualizaciones puntuales de su tabla. Las tablas se actualizan más rápidamente, así que los mensajes se difunden más rápido y las rutas se reestablecen antes.

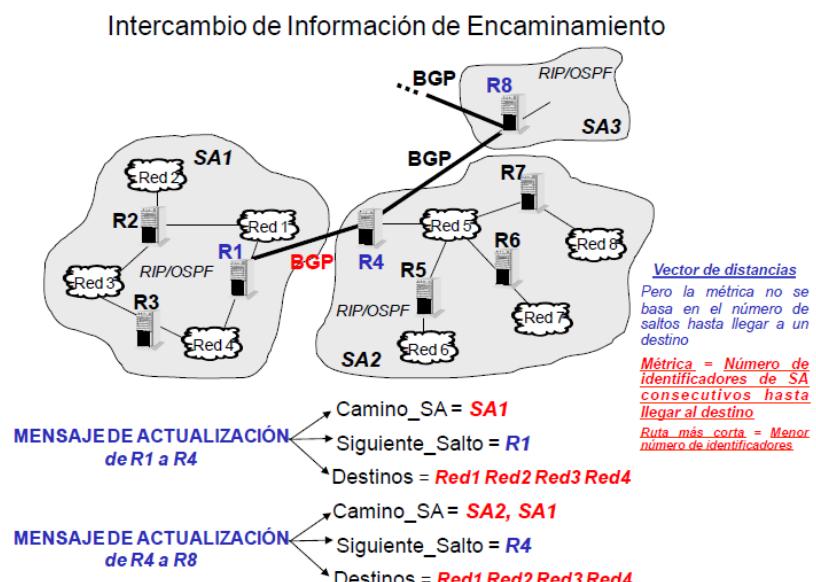
- **Métrica:** puede usar diferentes medidas como la capacidad de enlace, retardos, longitud de enlace, etc.
 - **Métrica de enlace:** asocia un mismo o diferente coste a cada enlace.
 - **Métrica total a un destino:** suma menor de los costes de cada enlace hasta llegar a destino.
- **Protocolo OSPFv4:** funciona en el nivel de red, con tipo de protocolo 89 en la cabecera IP. Un router OSPF dispone a través de mensajes OSPF la ruta completa de routers. Se usa en topologías de todos los tamaños. La sobrecarga es baja ya que las actualizaciones informan de los cambios y no de todas las rutas de la tabla a la vez. Vía OSPF permite a los routers cambiar dinámicamente las rutas en función de la sobrecarga de tráfico de éstas e incluso balancear o distribuir la carga de paquetes entre rutas alternativas a un mismo destino. Es seguro igual que RIPv2.

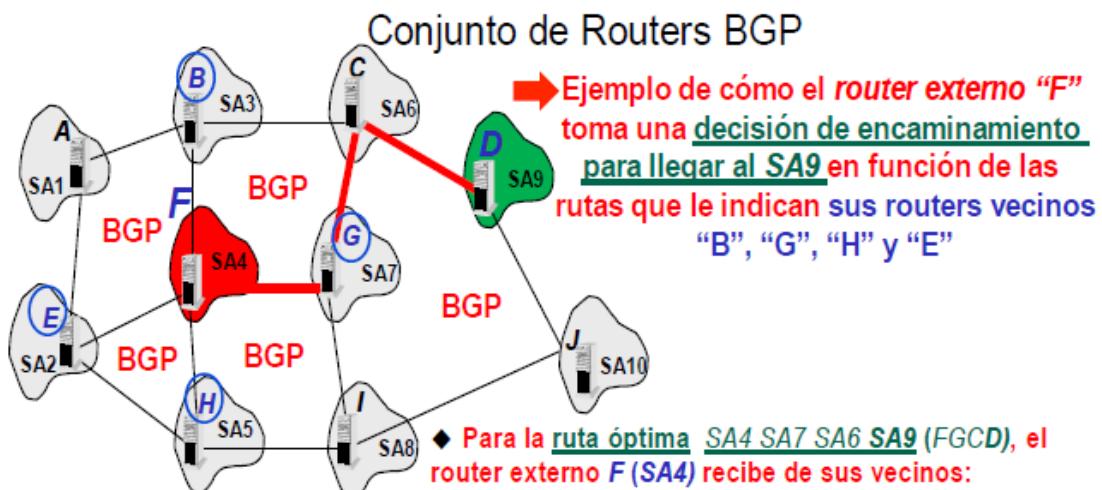


Cuando un router se acerca a su umbral de congestión avisa a los routers vecinos con un mensaje OSPF de congestión. Inmediatamente esos routers actualizan su tabla IP para ajustarse a una nueva ruta que evite el router congestionado.

❖ **Protocolo EGP BGP-4:** funciona sobre TCP, puerto 179.

- **Métrica:** no es el número de saltos sino el número de identificadores de sistemas autónomos consecutivos hasta llegar a destino. Un router BGP dispone de la topología completa o itinerario de sistemas autónomos. No se guarda solo el siguiente salto a un destino sino la ruta completa evitando que se formen bucles.





Ejemplo de cómo el **router externo "F"** toma una decisión de encaminamiento para llegar al **SA9** en función de las rutas que le indican sus routers vecinos "B", "G", "H" y "E"

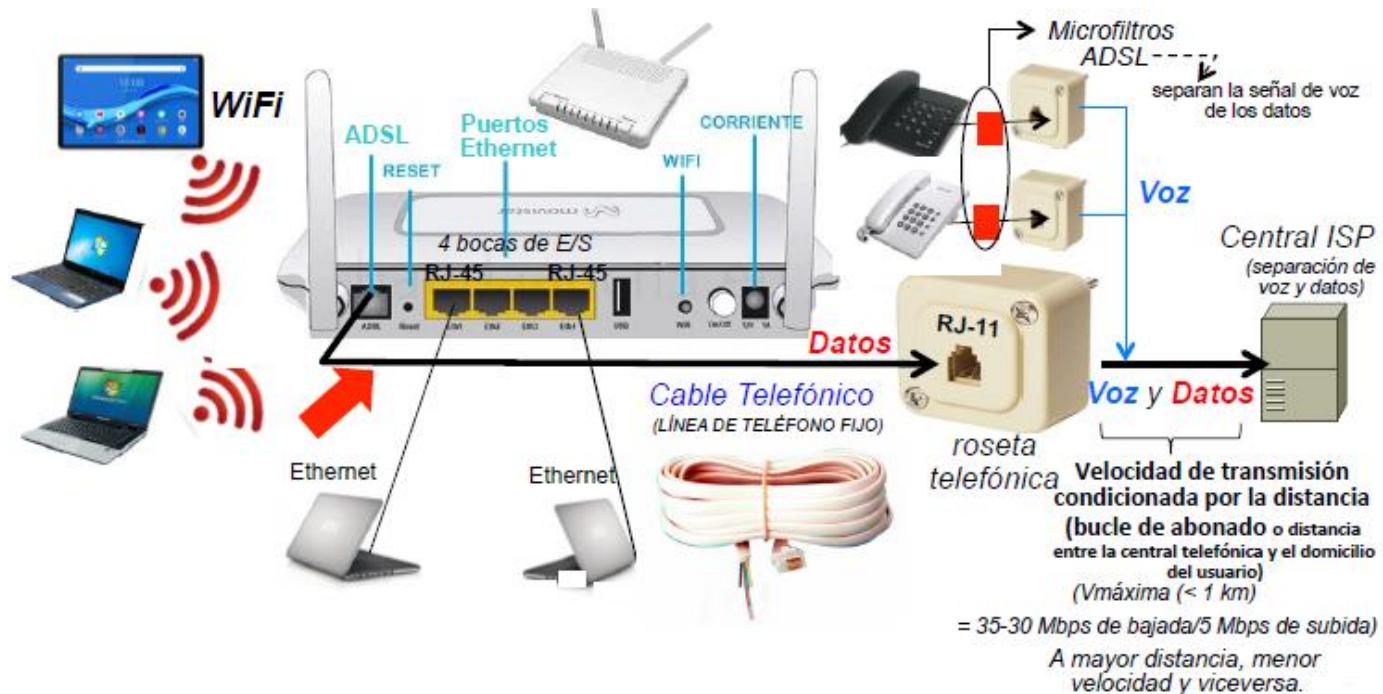
◆ Para la ruta óptima **SA4 SA7 SA6 SA9 (FGCD)**, el router externo F (SA4) recibe de sus vecinos:

- ✓ De B: SA3 SA6 SA9
- ✓ De G: SA7 SA6 SA9
- ✓ De H: SA5 SA4 SA7 SA6 SA9 (ruta descartada al pasar a través de SA4)
- ✓ De E: SA2 SA4 SA7 SA6 SA9 (ruta descartada al pasar a través de SA4)

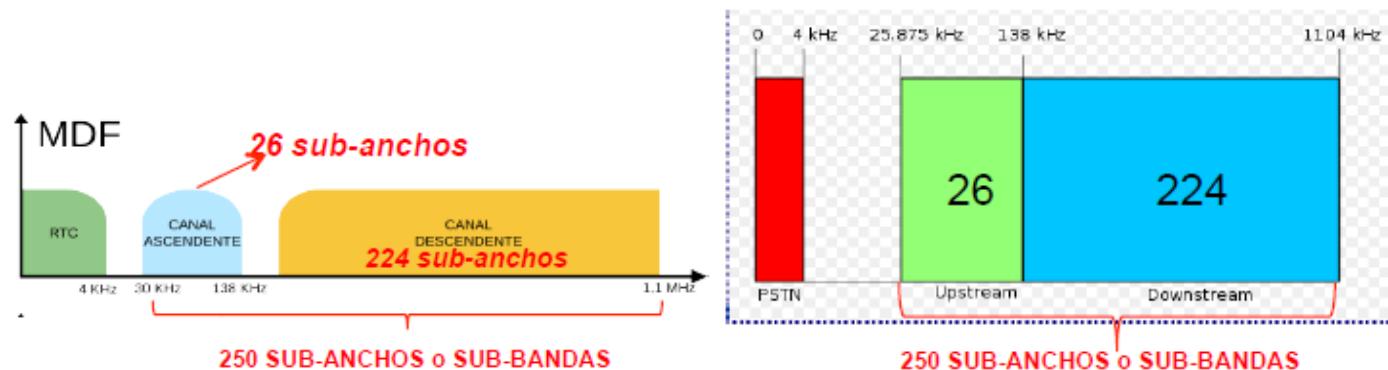
LA DECISIÓN CONSISTIRÁ EN PASAR POR **SA3 (SA3 SA6 SA9)** o **SA7 (SA7 SA6 SA9)** DEPENDIENDO DE LA POLÍTICA DE ENCAMINAMIENTO

5.2 TECNOLOGÍAS DE ACCESO A INTERNET

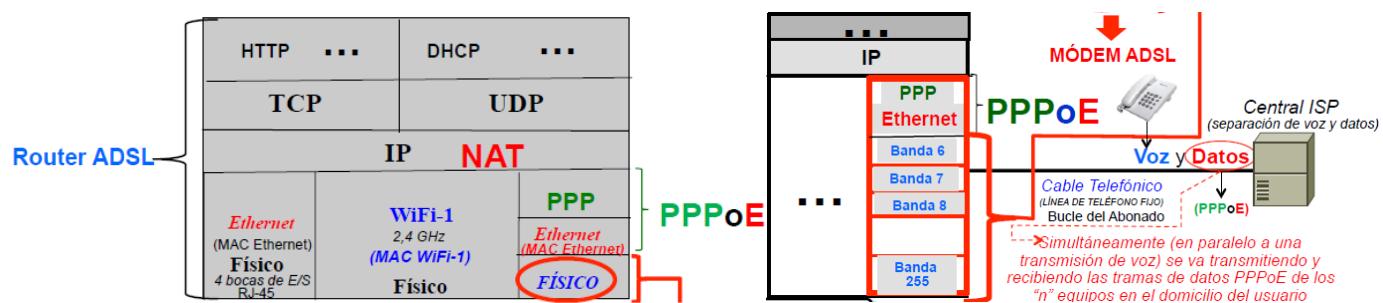
ADSL (Asymmetric Digital Subscriber Line): tecnología de Acceso a Internet a través de un cable telefónico de cobre sin interferir con las conversaciones telefónicas, de tal forma que se pueda hablar telefónicamente mientras se está conectado a Internet. Para ello el cable telefónico se divide en tres canales: para llamadas, para descargas y para subidas.



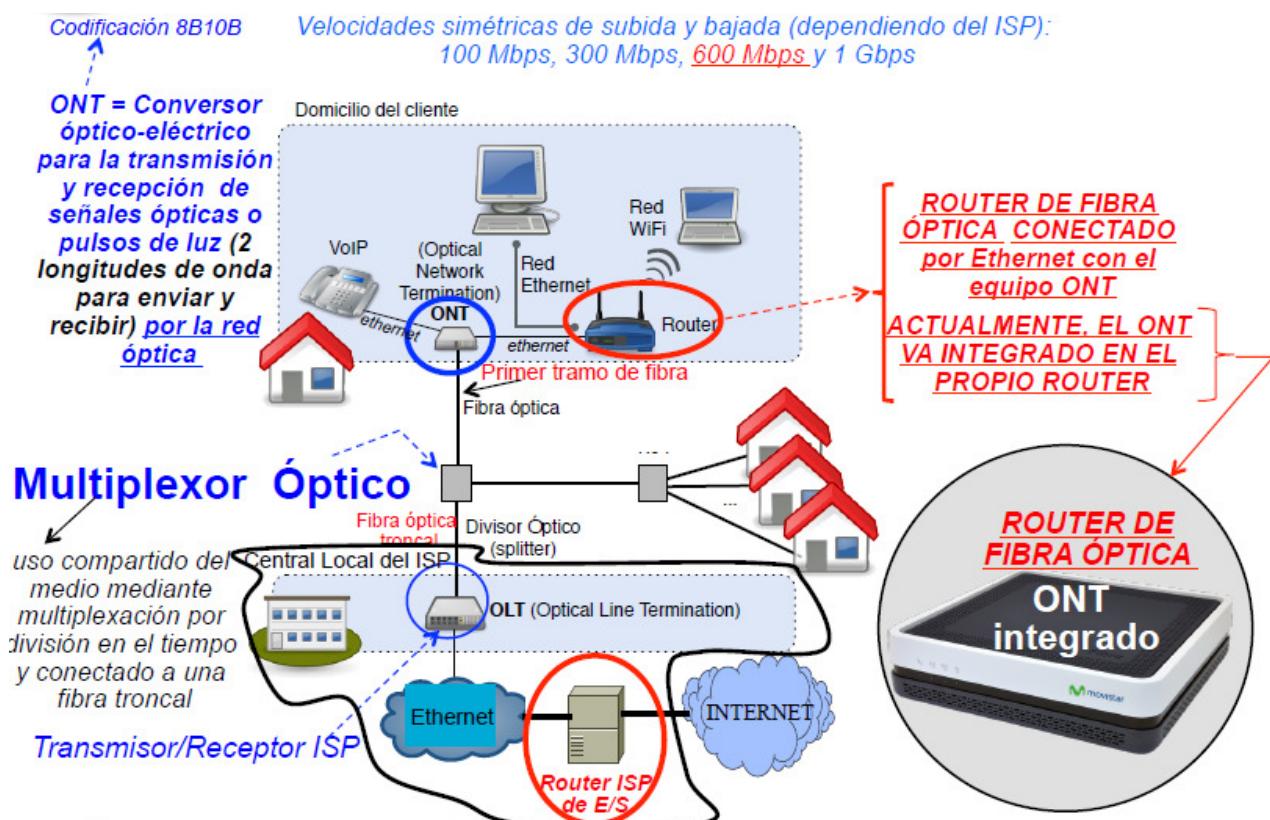
ADSL divide mediante modulación dicho ancho de banda de 1,1MHz en 256 canales de 4KHz. El canal 0 se utiliza para RTC (real time communication), los canales ascendentes para los datos que van desde el usuario hacia Internet y los descendentes para los que van de Internet al usuario. Los canales 1-5 no se usan para evitar interferencia entre voz y datos. La información baja multiplexada por frecuencia (MDF).



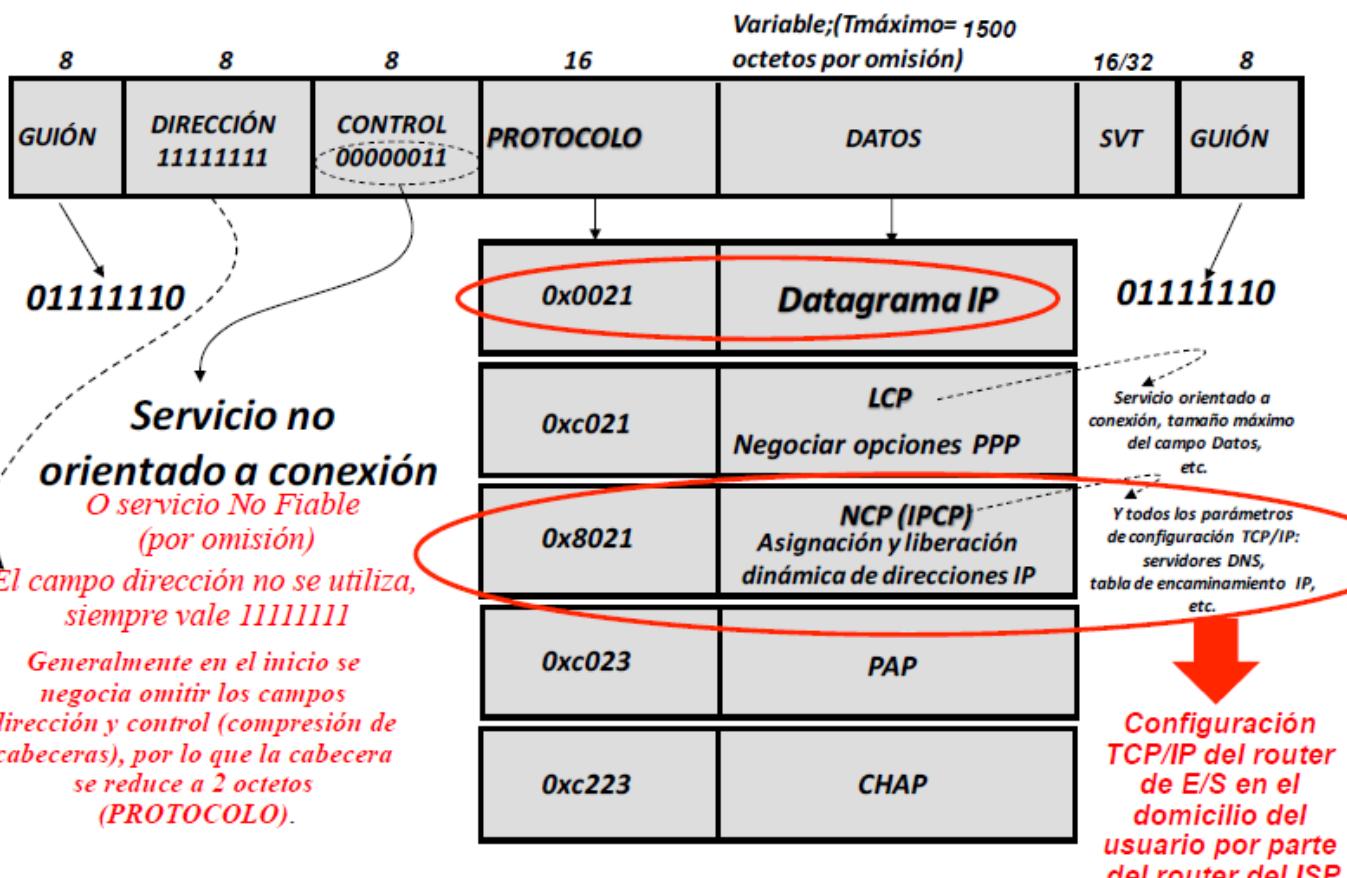
El router a nivel de enlace da soporte a Ethernet, WiFi y a PPP, que es un point to point sobre Ethernet. En la parte de los datos de la trama Ethernet viaja la información point to point.



Fibra óptica:



PPP: protocolo típicamente del nivel de enlace en líneas serie punto a punto (fibra óptica y ADSL). Puede ser directamente el protocolo de nivel de enlace o puede ir encapsulado en la trama Ethernet. Por omisión es no fiable, pero se puede configurar para que lo sea. El formato de trama cuando PPP no funciona sobre Ethernet es el siguiente:



Redes de telefonía móvil: según avanzan las generaciones aumenta el rango de frecuencias, las velocidades de transmisión y los chips son más eficientes y consumen menos recursos.

