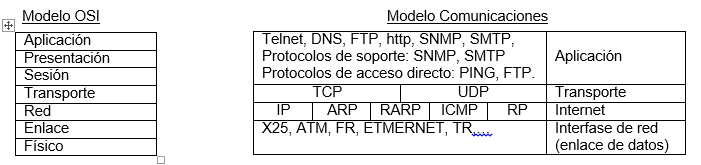
**Resumen Redes – 1º Parte**

# Introducción

## Modelo OSI: Las funciones de comunicación se dividen y distribuyen entre las distintas capas, de forma que las capas superiores se apoyan en las inferiores.

1. **Física**: Responsable de la interfaz física entre los dispositivos. Define reglas para la transmisión de los bits.
2. **Enlace**: Responsable de transferencia de datos seguros a través del enlace físico, envía las tramas, sincroniza, mantiene el control del enlace (conecta, desconecta, mantiene). Su principal objetivo es la detección y control de errores.
3. **Red**: Su objetivo es hacer que los paquetes lleguen destino y mantener las conexiones. Proporciona independencia a las capas superiores respectos a las técnicas para conectar a los sistemas
4. **Transporte**: Proporciona seguridad para el envío de los datos entre los aplicativos, asegura que los datos lleguen correctamente. Puede estar involucrada en la optimización del uso de red y en proporcionar calidad de servicio solicitada
5. **Sesión**: Responsable del control de comunicación entre las aplicaciones, maneja las sesiones entre las distintas aplicaciones, permite recuperación de errores.
6. **Presentación**: Independiza la aplicación respecto de la representación de los datos.
7. **Aplicación**: Proporciona a los usuarios el acceso a OSI.



# Protocolo de comunicaciones

## Funciones:

1. **Encapsulamiento (trama)**: De la “Información a Enviar” + los “Datos de control” en un PDU (Unidad de Datos del Protocolo).
2. **Segmentación y Ensamblado**: Para grandes volúmenes de datos, estos se parten y se ensamblan en distintos paquetes. Según el tamaño, se obtienen distintas características en la comunicación.
   * Menor PDU:
     + Más eficiente el control de errores
     + Menos memoria (buffer)
     + Menos necesidad de interrupciones
     + Más información adicional relativa
   * Mayor PDU:
     + Mayor eficiencia de transmisión
3. **Control de la conexión**: mediante mecanismos para abrir / transferir / cerrar conexiones.
4. **Control de flujo:** para determinar el momento en el cual enviar (o no) información, y no sobrecargar la memoria temporal de transferencia del dispositivo receptor. Pueden ser mediante Parada y Espera (|) o Ventana Deslizante (||).
   * Tiempo de transmisión: tiempo empleado para emitir todos los bits de una trama al medio.
   * Tiempo de propagación: tiempo empleado por 1 bits en atravesar el medio de transmisión.

## CONTROL DE FLUJO: Sucede en la Capa de Transporte, por lo cual tendremos que identificar como lo realiza el protocolo TCP versus el protocolo UPD

## Control de Flujo – Parada y Espera [Stop and Wait]

* *Método más sencillo. El emisor envía una trama, el receptor recibe y envía confirmación (ACK – Caso contrario es un NAK) por cada una de las tramas enviadas, solo si esta ocurre el emisor puede seguir emitiendo. Sólo puede haber una trama en tránsito por vez.*
* *CASO ÓPTIMO: Cuando se envían pocas tramas y de gran tamaño.*

*- USO: Poco frecuente. El origen tiende a fragmentar la información en bloques pequeños, debido al tamaño limitado del buffer (memoria temporal) del receptor.*

*- COMPLICACIONES: Si hay error se debe retransmitir mayor cantidad de datos; una estación ocuparía mucho tiempo el medio de transmisión.*

***Control de Flujo******- Ventana deslizante [Sliding Windows]***

* *RQ Continua (dúplex)*
* *Envía X cantidad de bloques sin esperar conformidad.*
* *En todas aquellas situaciones en las que la longitud del enlace en bits sea mayor que la longitud de la trama (alfa > 1) habrá problemas de ineficiencia.*

***Control de Flujo*** *-* ***Piggyback***

*A le envía a B. B le envía un paquete a A y lo aprovecha para enviar ahí dentro el NAK / ACK de lo que había recibido.*

*Ambas partes envían datos y confirmaciones.*

1. **Entrega ordenada**: Permite que las PDU lleguen en el orden que fueron enviadas o que dicho orden pueda verificarse en el receptor y generarse.
2. **Direccionamiento**: A través de la dirección IP puede encontrar el host destino y a través de la dirección de puerto (SAP) puede encontrar a la aplicación destino.
3. **Control de errores**: mediante la Detección y el Reenvió de las tramas.
4. **Multiplexación**: de distintas conexiones lógicas sobre una única física.

# CAPA FÍSICA (7 de 7) | CAPA Interfaz de Red (1 de 4)

**Objetivo**: Codificación/decodificación de señales, tratamiento de preámbulo, transmisión y recepción de bits. Incluye una especificación del medio de transmisión y la topología.

## Dispositivos de red:

* **HUB [Capa 1 - Física]**: regenera y re temporiza la señal de red para permitir que la información viaje a mayor distancia a través de los medios (longitud máxima del enlace es de 100m). cada estación tiene dos cables uno para transmitir y otro para recibir.

# CAPA – ENLACE DE DATOS (6 de 7) | CAPA Interfaz de Red (1 de 4)

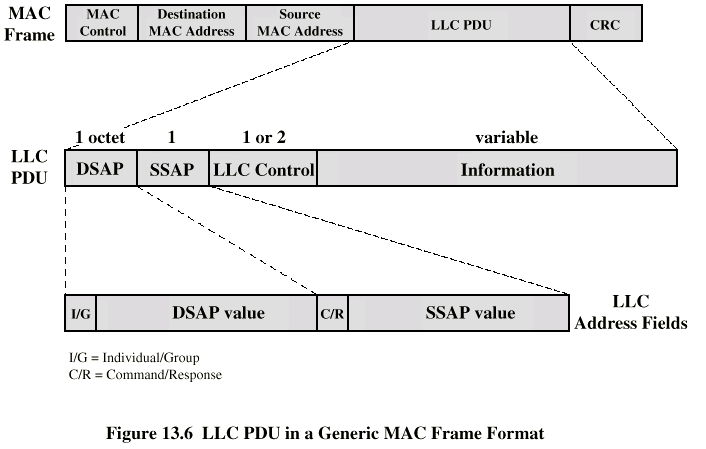
## Dentro de la capa de Enlace de Datos, encontramos que se encuentra divida en dos secciones:

## Sub Capa - Control de Enlace Lógico (LLC)

* Proporciona a la capa superior (RED), una interfaz independiente de la tecnología usada para enlace de Datos. Participa en el proceso de encapsulamiento.
* Recibe el paquete IP, y le agrega dos componentes de direccionamiento: el Punto de Acceso al Servicio Destino (DSAP) y el Punto de Acceso al Servicio Fuente (SSAP).
* Modos operativos:
  + **Modo orientado a conexión, con numeración de la secuencia de tramas**. Se establece conexión lógica entre usuarios y hay un control de flujo y de errores.
  + **Modo no orientado a conexión y sin confirmación:** Permite unicast, multicast, broadcast. Servicio tipo datagrama, no incluye control de flujo ni errores, no garantiza recepción de datos, esto queda a manos de capas superiores.
  + **No orientado a conexión con confirmación**: los datagramas son confirmados pero no se establece conexión lógica previa entre los usuarios.

## Sub Capa - Control de Acceso al Medio (MAC)

* En transmisión, participa en el ensamblado de datos en tramas y de la detección de errores.
* En la recepción, participa en el desensamblado de tramas y la detección de errores.
* Tipos:
  + **Centralizado / Descentralizado**: Existe un controlador que otorga permiso al medio. O, las estaciones realizan el trabajo de control de acceso juntas y dinámicamente.
  + **Síncrono/ Asíncrono**: le da un espacio fijo a cada host. O, cambia dinámicamente según la necesidad
  + **Circular**: A cada estación se le asigna el turno y si quiere transmite, luego el turno se cede a la estación siguiente.
  + **Reserva/ Competencia**: Se reserva un espacio para la transmisión. O, las estaciones compiten por la transmisión.



## Dispositivos de red:

### Puente Bridge [Capa 2 - Enlace]:

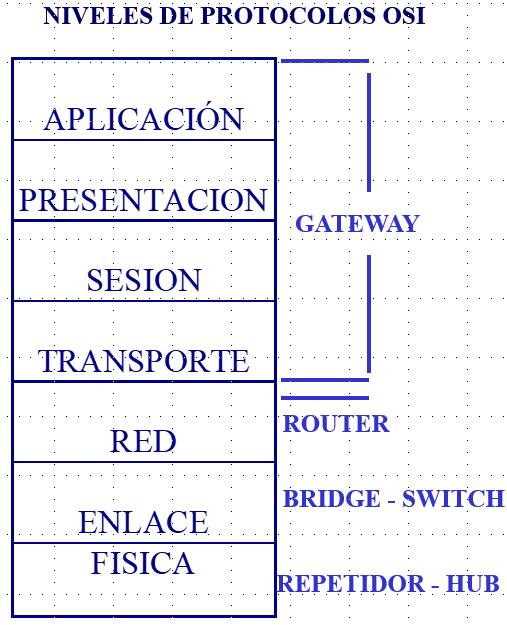
* + Dispositivo que interconecta dos o más Redes LAN, posee una función similar al repetidor.
  + Almacena y hace control de errores antes de retransmitir las tramas MAC. No sobre carga a la red
  + **Puente Transparente (Transparent).**
    - Dispone de memoria y aprenden automáticamente la ubicación de los hosts.
    - Las tramas soportan dos procesos: Direccionamiento y Enrutamiento (“Filtering y Forwarding”)
  + **Puente Translúcido (Translating)** 
    - Adiciona la conversión de protocolo y Velocidad.

### Conmutador Router [Capa 2 - Enlace]:

* + Permite interconectar dos o más segmentos de red. Si se encuentra en la Capa 3 – Red, permite interconectar dos o más subredes.
  + No mantiene completamente ocupado al medio como en el caso de los HUB.
  + Se encarga de armar una tabla de ruteo, se hacen transferencias paralelas y maneja colisiones con un par dedicado UTP.

### Switch [Capa 2 - Enlace]:

* + Multiplica la capacidad de la red LAN (capa 2).
  + Permite que más de una estación transmita por vez.
  + Los dispositivos conectados por switchs de capa 2 tienen direccionamiento plano (MAC). Todos comparten la dirección MAC para difusión.
  + Si un dispositivo envía una trama de difusión, se entrega a todos los conectados por el switch y/o bridges



## Direcciones Unicast, Multicast y Broadcast

* **Unicast**: identifica a una sola estación.
  + El primer byte (dos dígitos) de la dirección MAC es un número par en decimal, por ejemplo: f2:3e:c1:8a:b1:01 es una dirección unicast porque “f2” (242) es un número par.
* **Multicast**: identifica a varias estaciones en forma simultánea (un frame es recibido por varias terminales).
  + El primer byte de la dirección MAC es un número impar en decimal, por ejemplo: 01:00:81:00:01:00 es multicast pues “01” (1) es un número impar.
* **Broadcast:** identifica a todas las estaciones de la red.
  + Tiene todos los 48 bits en uno (ff:ff:ff:ff:ff:ff:).
  + Una dirección Broadcast es un caso especial de dirección Multicast.

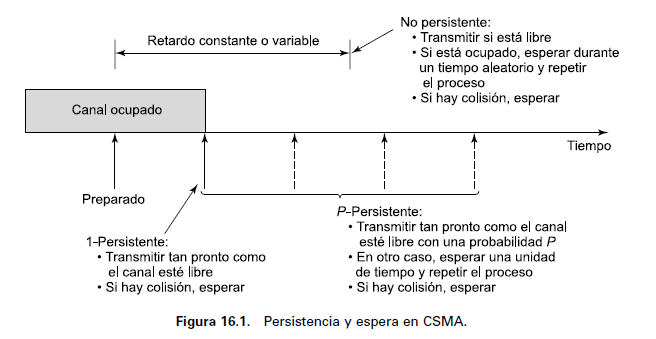
## Protocolos para el Control de Acceso al Medio: Arbitran la utilización del canal de difusión. Existen grandes tipos, de acceso aleatorio (no se sabe cuándo se va a requerir el canal) y contención (los equipos compiten por el medio).

### Aloha: Para redes de LAN. Posee un alto nivel de colisión y las estaciones transmiten las tramas SIN escuchar al medio

* + **Aloha puro:** Las estaciones comparten el mismo canal.
  + **Aloha ranurado**: Transmiten en determinado instantes de tiempo (existen “ranuras” o canales diferidos), de este modo el número de colisiones es menor. Cada estación solo puede transmitir al principio de una “ranura”.

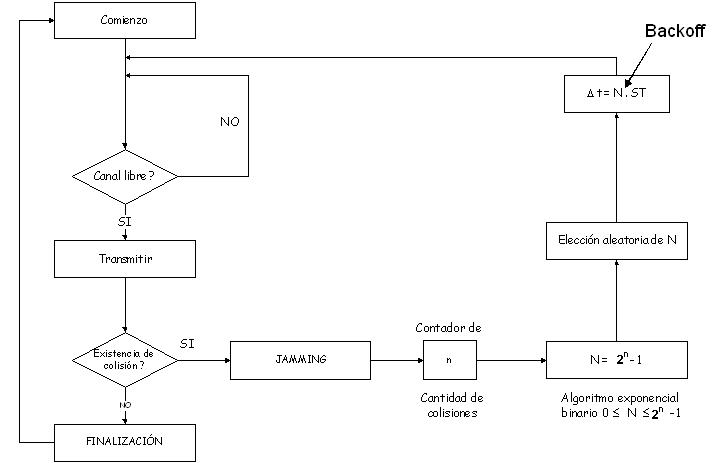
### CSMA /CA: Los dispositivos ESCUCHAN si el medio se encuentra libre. Si está ocupado o hay colisión esperan X tiempo. Se utiliza en redes inalámbrica.

* + **No persistente**: Esperar una cantidad de tiempo aleatorio e intentar transmitir.
  + **1-Persistente**: Transmitir tan pronto como el canal esté libre.
  + **P-Persistente**: Transmitir tan pronto como el canal esté libre con una probabilidad P y se esperar una cantidad de tiempo (1-P).



### CSMA/CD: Soluciona el problema del que el medio permanece inutilizable ante una colisión. Se utiliza en ETHERNET II.

* + - Si el medio se encuentra libre, transmite. Si el medio se encuentra ocupado, continúa escuchando hasta que el canal se libere, en cuyo caso transmite inmediatamente (1-Persistente).
    - Si se detecta una colisión, se transmite una pequeña señal de interferencia para que todos se enteren de la colisión y deja de transmitir. La estación espera una cantidad aleatoria de tiempo conocida como espera (BACKOFF).
      * **Algoritmo exponencial binario:** Sirve para calcular el tiempo de espera posterior a la colisión (BACKOOF), en base a un algoritmo exponencial (2^n -1)
        + ST: Slot Time, es el tiempo para propagar 512 bits, 51,2 microsegundos en 10 Mbps.
        + n: Cantidad de colisiones, con un valor máximo de 10 (se repite 6 veces).



*Datos:*

**ST -Slot Time**: Tiempo en transmitir 512 bits (trama corta).

***PT (Propagation Time)****: Tiempo de propagación entre las estaciones más lejanas (Ida).*

***RTT (Round Trip Time)****: Tiempo de Ida y Vuelta (2xPT).*

***RTTmax****: Ventana de colisión.*

*T para detección de colisiones < RTT Max.*

*Errores en la transmisión ocurren por ruido en el canal o colisión de tramas.*

Anillo con paso del testigo:

Definido en el estándar 802.5 propone una LAN con topología de anillo, la cual utiliza una pequeña trama, llamada testigo, para controlar el acceso al medio. El funcionamiento es el típico del anillo, pero para transmitir, una estación debe esperar que le llegue el testigo, el cual va girando por el anillo y es tomado antes de transmitir y liberado luego de haber transmitido.

## Ethernet II | Ethernet 802.3

A) Protocolo de Acceso al Medio (MAC): CSMA/CD

* ***Ethernet 802.2 - DIX v2*** *(Si el campo Tipo Ethernet > 05DC [1500])*

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **7 bytes** | **6 bytes** | **6 bytes** | **2 bytes** | **46 - 1500 bytes** | **4 bytes** |
| **PREAMBULO** | Dir. Destino | Dir. Origen | Tipo\_Trama | LLC Data | FCS |

**Tipo Ethernet**: En forma codificada indica el protocolo de red que se está utilizando. Por ejemplo: IPv4 - 0800, IPv6 - 86DD y ARP - 0806

* ***Ethernet 802.3*** *(Si el campo Longitud < 05DC [1500])*

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| **7 bytes** | **1 byte** | **6 bytes** | **6 bytes** | **2 bytes** | **46 - 1500 bytes** | **4 bytes** |
| **PREAMBULO** | SFD | Dir. Destino | Dir. Origen | Longitud\_Trama | LLC Data | FCS |

* + *Preámbulo: 7 octetos de bits 0 y 1 alternados para establecer sincronización y anunciar la trama.*
  + *Start frame Delimiter: Secuencia de bits que indica comienzo real de la trama, para que el receptor pueda saber a partir de cuándo leer.*
  + **Destino**: estación que debe recibir la trama.
  + **Origen**: estación que envía la trama.
  + **Longitud o Tipo de Trama Ethernet**:
    - Longitud del campo de datos LLC en bytes, el tamaño máximo de la trama sin Preámbulo y SDF es de 1518 B.
    - Protocolo de red que se está utilizando.
  + **Datos LLC**: unidad de datos proporcionada por la sub-capa “Control de Enlace Lógic (LLC)”.
  + Relleno: bytes agregados para que la trama tenga el tamaño suficiente para la técnica de detección de colisiones.
  + **Frame Check Sequence**: comprobación de redundancia cíclica, calculada teniendo en cuenta los distintos campos excepto el preámbulo y SFD.

**Definiciones**

### Dominios de Colisiones:

* + Área de red dentro de la cual se pueden propagar colisiones, por ocupación simultánea del medio.
  + Cada puerto de Switch es un dominio de colisión.
  + Repetidores - Hubs [Capa Física]: SI propagan colisiones
  + Bridge, Switch y Routers [Capa Enlace y Red]: NO propagan colisiones.

### Dominios de Broadcast:

* + Área de red donde se propagan las tramas de difusión.
  + Está determinado por cada Router.
  + Conjunto de todos los dispositivos que recibirán frames de broadcast provenientes de cualquier dispositivo del conjunto.

## Protocolo STP “Spanning Tree Protocol” (IEEE 802.1D)

* **¿Función?:** 1 -Retransmisión de tramas | 2- Aprendizaje de direcciones para gestionar bucles en redes con enlaces redundantes.
  + 1ro – Selección del Switch ROOT | 2do – Establecen los puertos designados, como enlaces a los demás Switchs |
  + Cada Switch - Bridge mantiene y actualiza su Tabla de Encaminamiento, para cada LAN que tenga conectada.
  + Cuando se descubre un “Bridging Loop”, se desactiva las interfaces del vínculo redundante.
  + Cuando se desconecta una interfaz o un puerto cambia de estado, se ejecuta el protocolo nuevamente para volver a activar otras interfaces.

- ¿Como se producen los “bridging loop”? Por el desconocimiento de la existencia de otros bridging.

- ¿Cómo determina el camino más barato? Con la PRIORIDAD o la VELOCIDAD. En caso de igualdad la MENOR DIRECCIÓN MAC desempata.

- Cómo determina el Switch - ROOT? Se selecciona el que posee menor valor de Bridge ID (Prioridad del puente + MAC).

## Protocolo VLAN [IEEE 802.1Q]

Consiste en una red de ordenadores que se comportan como si estuviesen conectados al mismo SWITCH, aunque pueden estar en realidad conectados físicamente a diferentes segmentos de una red de área local.

* Posee un dominio de colisión por cada puerto de SWITCH.
* El dominio de Broadcast en único para todas.
* AIslan redes de acuerdo a la dirección MAC; IP, Puerto o Protocolo. Sin embargo, mediante los puertos TRUNK puedo hacer que las VLANs se interconecten, se requiere de un dispositivo de nivel 3 (Router).

|  |  |  |
| --- | --- | --- |
| Tipo\_Trama (0810) | Prioridad | Número de VLAN |
| 4p (16 bits) | 1p (3 Bits) | 3p (13 Bits) |

**Redes LAN Inalámbricas**

Modo Ad-hoc: Las estaciones se comunican directamente, sin requerir un punto de acceso; constituyendo un IBSS (red Wi-Fi).

Modo infraestructura: Se debe disponer de un Access Point, la red wifi de uso habitual.

*Una LAN inalámbrica debe cumplir los requisitos de una LAN común, y además de estos:*

* *Rendimiento: el protocolo de control de acceso al medio debe maximizar el uso del medio inalámbrico.*
* *Número de nodos: Puede tener que satisfacer la demanda de múltiples nodos.*
* *Conexión a LAN troncal: Es necesario que se conecte a esta.*
* *Robustez en la trasmisión y seguridad, funcionamiento de redes adyacentes.*

## WiFI [IEEE 802.11]

El estándar 802.11 posee una estructura celular, cada celda llamada Basic Service Set (BSS) está compuesta por estaciones que comparten el mismo protocolo de Control de Acceso al Medio (MAC) y compiten por él.

* Distribution System: LAN cableada que comunica los Access Point (Router).
* Access Point (Router): Estación base a la cual se conectan los terminales.
* Terminales: Son las estaciones que obtienen acceso a través de Acess Point.

|  |  |
| --- | --- |
|  |  |

*El estándar 802.11 se involucra en las capas inferiores del Modelo OSI:*

* *La capa física ofrece tres tipos de codificación de información (FH,DS y IR). Define modulación de las ondas de radio y las características de señalización para la transmisión de datos.*
* *La capa de enlace de datos compuesta por las subcapas Control de Enlace Lógico (LLC) y Control de Acceso al Medio (MAC) define la interfaz entre el bus del equipo y la capa física.*

### *Control de Acceso al medio (MAC):*

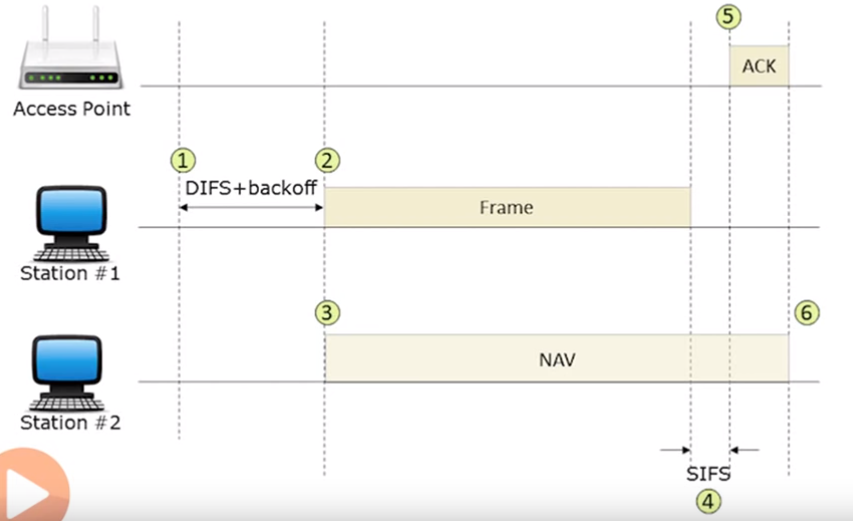
* **Entrega fiable de datos**: Toda trama enviada tiene que confirmarse (ACK) en un período de tiempo, o se retransmite.
* **No puede utilizarse CSMA/CD.** No incluye detección de colisiones (CD) porque no resulta práctico en una red inalámbrica. **Recordar que “CD” es Colission Detect**

**Función de Coordinación Distribuida (DCF)** [Utiliza CSMA/CA con intercambio de RTS/CTS y opcionalmente ACK]

Todos los equipos tienen una misma probabilidad de tomar el medio.

* 1. Terminal - Transmite solo si el medio está libre por un intervalo de tiempo determinado (IFS).
     + Si el canal está ocupado inicia un temporizador aleatorio (backoff), y transmite cuándo éste finalice.
     + El temporizador disminuye solo cuándo el canal está libre y aumenta con cada vez que NO recibe un ACK (envío fallido).
  2. Terminal - Transmite un RTS (Request to send) y “reserva el medio”
  3. Access Point - Recibe un RTS, y si el canal está libre envía un CTS (Clear to send- Estás autorizado para transmitir por X tiempo) => momento 0.
  4. Terminal: Recibe el CTS y trasmite las tramas.
  5. Access Point: Recibe los datos, verifica el CRC y después de un tiempo SIFS y envía un ACK => Momento 1.
  6. Terminal: Recibe el ACK de la recepción.
  7. El receptor recibe la trama, verifica el CRC y envía un ACK después de un SIFS

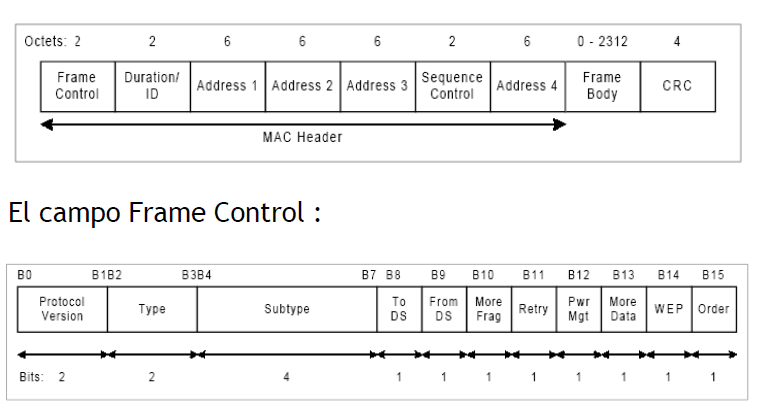
El tiempo ocurrido durante la transmisión (Momento 0 a 1) es denominado NAV.



* **Función de Coordinación Puntual (PCF)**: Similar a Token Ring, el Access Point va preguntando a cada equipo si tiene algo para transmitir. No es utilizado normalmente dado que PIFS es menor que DIFS este puede adueñarse del medio.

**Trama – Campo “Frame Control”**

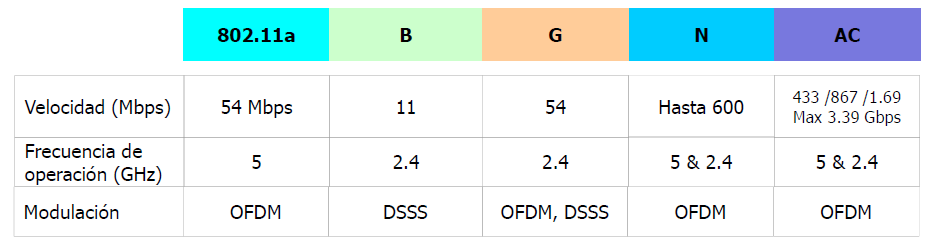
* Versión (2 bits): 0
* Tipo (2 bits):
  + **Gestión (00)**: Gestionan las comunicaciones entre las estaciones y los AP (Sincronización, Autenticación y Asociación).
  + **Control (01)**: Estas prestan servicio a la entrega fiable de datos (RTS, CTS y ACK).
  + **Datos (10)**: transportan los datos en sí del usuario (Datos, Datos + CF-ACK, Datos + CF-Poll y Datos + CF-ACK + Cf-Poll), existen 8 subtipos de tramas de datos, organizadas en dos grupos.
* Subtipo (4 bits): RTS - Petición de envió (1011) CTS – Libre para enviar (1100) | ACK - Confirmación(1101)
* To DS (1 bit): Indica si va al Distribution System (se define después)
* From DS (1 bit): Indica si viene del Distribution System (se define después)
* More Flag (1 bit): Indica si hay Más Fragmentos
* Reintento (1 bit): Indica si la Trama es retransmitida
* Gestión de potencia (1 bit): Indica en qué modo estará la estación después de transmitir
* Más datos (1 bit): Hay más datos para enviar
* WEP (1 bit): Cifrado implementado
* Rsvd (1 bit): Reservado



**Diferencias con Ethernet**:

* Debido a alto BER de la capa 1, conviene dividir los 1500 bytes de datos en fragmentos menores, y luego se transmitirán estos uno a continuación del otro.
* **Conexión requiere de 3 pasos: Sincronización con el medio, Autenticación y asociación entre el AP y el Terminal.**
* Para protección se usa el protocolo WEP para evitar la intercepción de información, y para limitar el acceso de los terminales a un determinado AP.

**Comparación con otros estándares**



# Protocolo - HDLC (High-level Data Link Control):

Características:

* *Es un protocolo de comunicaciones punto a punto/multipunto.*
* *Protocolo orientado al bit y sincrónico.*

***Estaciones:***

* *Primaria: sus tramas son órdenes. Responsable de controlar el funcionamiento del enlace.*
* *Secundaria: sus tramas son respuestas, funciona bajo control de la estación primaria.*
* *Combinada: combinación de las anteriores, puede generar órdenes o respuestas.*

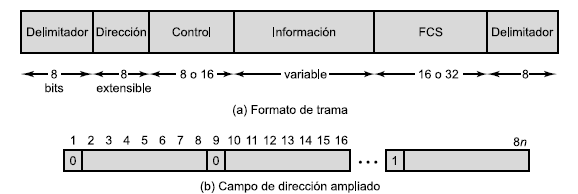
**Configuraciones de enlaces:**

* *No balanceada: está formada por una estación primaria y una o más secundarias, permite transmisión Full dúplex y Half dúplex.*
* *Balanceada: consiste en dos estaciones combinadas. Permite Half y Full Duplex.*

***Modos de transferencia de datos:***

* *Modo de respuesta normal (NRM): La estación primaria puede iniciar la transferencia hacia la secundaria, y la secundaria solo puede transmitir datos en respuesta a órdenes emitidas por la primaria [configuración no balanceada].*
* *Modo de respuesta asíncrono (ARM): la estación secundaria puede iniciar la transmisión sin permiso explícito de la primaria, aunque ésta sigue teniendo la responsabilidad del funcionamiento de la línea [configuración no balanceada].*
* *Modo balanceado asíncrono (ABM): Cualquier estación combinada puede iniciar transmisión sin haber recibido permiso previamente [configuración balanceada].*

**Estructura de trama:**



* **Delimitador**: Delimita el inicio de la trama. Siguen la forma (01111110), utiliza el mecanismo de inserción de ceros para garantizar transparencia, no debe existir en los datos una combinación de bits igual a la del FLAG.
* **Dirección**: Identifica a la estación origen o destino de la trama. El campo de dirección consta normalmente de 8 bits, si bien, tras una negociación previa, se puede utilizar un formato ampliado en el que la dirección es múltiplo de siete bits.
* **Control**: formato variable, se implementan mecanismos de control de flujo y enlace. Existen 3 tipos de tramas:

­



* + **Información** (I): Transportan los Datos generados por el usuario + Control de Flujo + Control de Errores
  + **Supervisión** (S): Se utilizan para el Reconocimiento y Aceptación de Tramas + Control de Flujo + Control de Errores. Adicionalmente, para la solicitud de transmisión o suspensión temporal de tramas. Tipos: “RR: Receptor Ready”, “RNR: Receptor No ready”, “REJ: Reject”, “SREJ: Selective Reject”.
  + **No** **numeradas** (U): Se utiliza para tareas de Conexión / Desconexión del enlace y Control del enlace.
  + *El Bit P/F tiene distintas funciones: Bit “P” – Solicitar respuesta de estado | Bit “F” – Finalización de trasmisión.*
* **Campo de información**: sólo presente en tramas de I - Información y en algunas U – No Numeradas. Cantidad de bits múltiplo de 8, es un campo variable.
* **FCS (Frame Check Sequence):** código para detección de errores (sin incluir delimitadores). Normalmente usa CRC de 16b.

**Conexión.**

1. **Establecimiento de conexión**:

* Lo puede solicitar cualquiera de los dos extremos en base a una transmisión de orden (existen 6). Si el otro extremo acepta, transmitirá una trama de confirmación (U) No numerada, si se rechaza se envía una trama de modo desconectado DM.
* Paso 1 - Avisar al otro extremo sobre la solicitud de iniciación,
* Paso 2 - Especificar el modo de transmisión (NRM, ABM, ARM),
* Paso 3 - Indicar como se van a usar los números de secuencia (3 o 7 bits).

1. **Transferencia de datos**: una vez iniciada la conexión se intercambian datos a través del uso de tramas de información (I).
2. **Desconexión:** Cualquiera de los extremos HDLC puede iniciar desconexión, tanto por haber detectado un fallo o por pedido de capa superior, se lleva a cabo al usar la trama DISC, la entidad remota respondería con (U) No Numerada.

**Control de flujo - Piggybacking**

Piggybacking es una técnica de transmisión de datos bidireccional, que envía el ACK de las tramas recibidas en la trama de información enviada como respuesta.

* Ventajas: Eficiente al disminuir el flujo de paquetes.
* Desventajas: El receptor podría retrasar el envío de ACK si no tiene datos que enviar. Se subsana con la incorporación de un “timer” en ambos extremos (en el emisor permitiría el reenvío de la trama y en el receptor permitiría el envío de un ACK individual).

**Control de errores.**

* **Mediante el campo FCS (Frame Check Sequence).**

*Derivados del HDLC:*

* *LAP-B (Link Access Procedure – Balanced): definido como parte de X.25. es un subconjunto de HDLC. Proporciona solo modo ABM. Diseñado para enlaces punto a punto entre el sistema usuario (DTE) y el nodo de una red de conmutación de paquetes (DCE), formato de trama idéntico HDLC.*
* *LAP-d (Link Access Procedure – D Channel): forma parte de recomendaciones ISDN. Proporciona el procedimiento de control de enlaces de datos sobre canal D. proporciona sólo modo ABM. Usa números de secuencia de 7 bits, campo de dirección de 16 bits.*

**Conexión:** Orientado a la conexión

# Frame Relay

Surge como solución a los problemas de X25: Su protocolo de control de enlace, al hacer control de flujo y errores, intercambia tramas de datos y de confirmación en cada salto a través de la red, y además los nodos intermedios deben guardar una tabla de estados por circuito virtual para ser utilizada luego.

* Derivado del HDLC. para eliminar la sobrecarga de procesamiento (x25),
* Alta velocidad y baja latencia al eliminarse el control de errores salto a salto.
* Se reemplaza VC (circuito virtual) de X.25 por DLCI (Data Link Connection Identifier)

**Conexión**: Orientado a la Conexión.

**Control de Errores / Congestión**: Las estaciones terminales dan cobertura de errores y flujo, necesitan una mayor inteligencia, las intermedias sólo transmiten.

* No hay recuperación de errores, si detección de errores y descarte de cuadros fallidos en los extremos. Existe un único tipo de trama para el transporte de datos de usuario.
* La congestión se controla con FECN y BECN.
  + FECN: Notificación explícita de congestión hacía delante.
  + BECN: Notificación explícita de congestión hacía atrás.
* Los POP setean estos bits y, los CPE y el administrador de la red los detectan

**Control de Flujo**

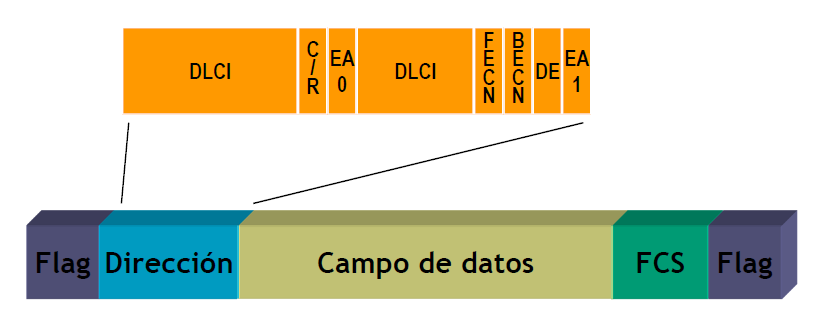
Se da mediante datos elegidos para descarte DE (Indicador de posible descarte): Bit establecido que indica que la trama se puede descartar para darle prioridad a otras tramas si se produce congestión. Cuando el router detecta congestión de red, el switch Frame Relay descarta en primer lugar los paquetes con el bit DE. El bit DE se establece en el tráfico sobresuscrito (es decir, el tráfico recibido después de alcanzar la CIR).

* **Bc (Ráfaga comprometida)**: Es la cantidad máxima de bits que la red garantiza su entrega, durante un tiempo Tc.
* **Tc**: Intervalo de tiempo durante el cual se mide la tasa de transmisión.
* **CIR (Caudal Mínimo Comprometido)**: Tasa de transmisión, en bits por segundo, que la red garantiza transmitir, bajo condiciones normales. => **CIR = Bc / Tc [DE=0]**
* **Be (Ráfaga en Exceso)**: Es la cantidad máxima de bits, por encima del CIR, que la red intentará transmitir durante un tiempo Tc. No hay un compromiso por la trasferencia de estos datos.
* **EIR (Ráfaga en Exceso):** Tasa de transmisión, en bits por segundo, en exceso => **EIR = Be/Tc [DE=1 – Indica que los paquetes se pueden descartar en caso de congestión]**
* **Las tramas enviadas por arriba del caudal de EIR serán directamente descartadas.**

|  |  |  |
| --- | --- | --- |
|  |  |  |

<https://ingteleco.webcindario.com/Redes/Transparencias/Tema%208%20-%20Frame%20Relay.pdf>

**Formato de Trama**



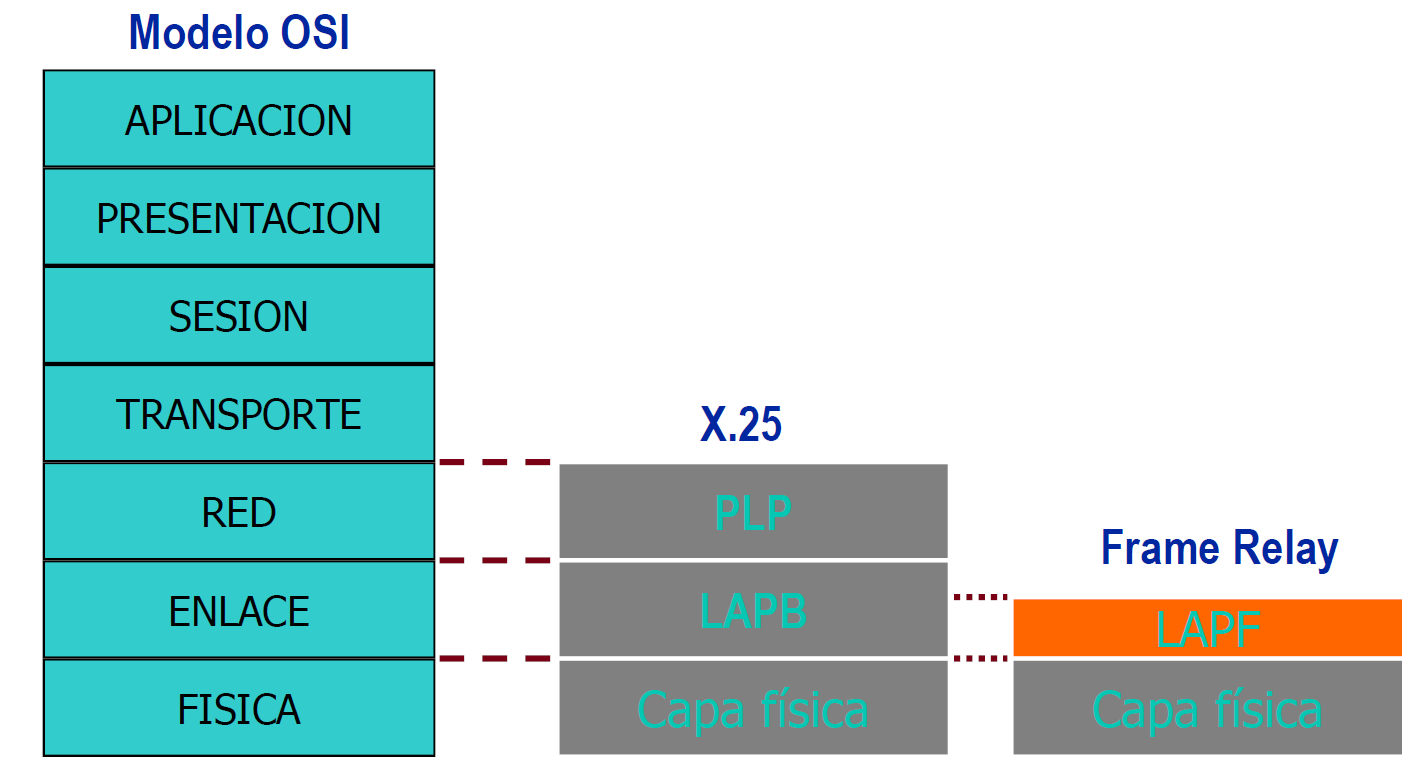
* **Flag [1 byte]: Correspondiente a secuencia 01111110 (7E).**
* **Dirección [2 byte]: 2, 3 o 4 bytes.**
  + **DLCI [6]: Identificador conector de linkeo de datos. Permite la multiplexación de varias conexiones lógicas de retransmisión a través de un único canal.**
  + **C/R [1]: Bit de orden/respuesta.**
  + **EA0 [1]: Bit de ampliación de campo de Dirección.**
  + **DLCI [4]: Identificador del circuito virtual.**
  + **FECN [1]: Notificación explícita de congestión hacía delante.**
  + **BECN [1]: Notificación explícita de congestión hacía atrás.**
  + **DE [1]: Conveniencia de rechazo.**
  + **D/C [1]: Identificador DLCI o control DL cen1tral.**
* **FCS - Frame Check Sequence [2 byte]: código para detección de errores (sin incluir delimitadores). Normalmente usa CRC de 16b.**
* **Flag [1 byte]: Correspondiente a secuencia 01111110 (7E).**

**Se consideran dos planos diferentes de operación:**

* **Plano “C” de control**: relacionado con el establecimiento y liberación de las conexiones lógicas, se implementan entre el usuario y la red.
* **Plano “U” de usuario:** responsable de la transferencia de los datos entre los usuarios que provee funcionalidad de extremo a extremo.

# DIFERENCIAS X25 - Frame Relay - ATM

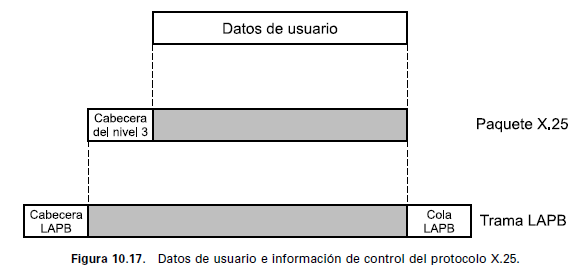
|  |  |  |  |
| --- | --- | --- | --- |
|  | **Frame Relay** | **X.25** | **ATM** |
| **Capacidad** | 1.5 Mbps | 64 kbps. | 10-100 Mbps |
| **Servicio** | Orientado a la conexión.  Ancho de banda: Por demanda. | Orientado a la conexión.  Ancho de banda: Fijo. | Orientado a la conexión.  Ancho de banda: Por demanda. |
| **Modelo OSI** | Niveles 1 y 2 (multiplexación y conmutación) | Niveles 1,2 y 3 (multiplexación y conmutación) | Nivel 2 (multiplexación y conmutación) |
| **Control de errores** | Detección – SIN corrección.  Nodo intermedio puede descartar.  Los externos solicitan el reenvío. [LAP-F | [LAP-D] | Detección + Corrección.  Nodo intermedio puede chequear y solicitar reenvío.  [LAP-B] | En cabecera (HEC), con capacidad para corregir 1 error. Transmite en enlaces altamente fiables. |
| **Control de Congestión** | Campos FECN, BECN y DE | Control de flujo por Ventana deslizante + PiggyBack | CLP: La celda se puede descartar en caso de congestión. |
| **Calidad de Servicio** | SIN calidad de servicios.  Caminos virtuales permanentes. | Con calidad de servicio.  Caminos virtuales + Canales lógicos | Camino y Canales virtuales. |
| **Información** | Ráfagas de paquetes | Paquetes. | Celdas de tamaño fijo. Transportadas en canales sincrónicos. Sin sincronizar. |
| **Caudal** | Garantizado entre 8 y 1984 Kbps | A mayor tráfico de red, menor eficiencia y mayor tiempo de respuesta. | A menor tiempo de respuesta, mayor eficiencia. |
| **Tipo tráfico** | Datos + voz | Datos | Datos + Voz + Video |



# X.25

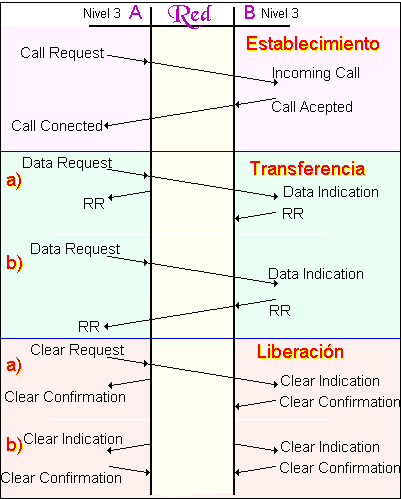
En la trama LAPB:

* El paquete X.25 se transporta dentro del campo de control, de tipo Información (I).
* Se encarga de que lleguen correctamente los paquetes X.25 que se transmiten a través de un canal susceptible de errores, desde o hacia la interfaz ETD/ETCD.



**La transferencia de los datos** se produce como con las llamadas virtuales, pero en este caso no se necesita realizar ni el establecimiento ni el cierre de la llamada.

* **Establecimiento:** El DTE que inicia la apertura de la conexión construye un paquete CALL REQUEST y se lo pasa a su DCE. La subred se lo pasa al DCE destino quien lo entrega al DTE correspondiente. Si este último acepta la llamada devolverá un paquete CALL ACCEPTED que llegará al DTE origen como CALL CONNECTED.
* **Transferencia**: La siguiente fase consiste en el uso full-dúplex del CV para intercambiar datos.
* **Liberación**: Cuando uno de ellos quiere terminar envía un paquete CLEAR REQUEST al otro extremo quien se lo confirmará con un paquete CLEAR CONFIRMATION.



**Control de flujo por Ventana deslizante + PiggyBack**

**Control de Errores - ARQ con vuelta atrás N**: basada en el control de flujo con ventana, en el caso de que un receptor detecte una falla en la trama X, dejará de aceptar tramas y enviará un REJ (Reject) al emisor, con lo cual este deberá retransmitir X y las siguientes que hayan sido transmitidas.

***Trama de red:***

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| GFI | LCI | TPI | ADD | FAC | Datos |
| 4bits | 12 bits | 8 bits |  |  |  |

* GFI: Secuencia de numeración de paquetes.
* LCI: Número de canal lógico.
* TPI: Tipo de paquete: llamada, supervisión, confirmación, interrupción, control de flujo.
* ADD: Plan de numeración.
* FAC: cobro revertido, grupo cerrado de usuarios, selección rápida, negociación de tamaño de paquete
* Campo de datos de usuario de llamada: identifica protocolo superior

# ATM (Modo de Transferencia Asíncrono):

**Características**:

* **Modelo OSI – Nivel 2. La capa ATM se encarga del multiplexaje y conmutación de celdas.**
* Mínima capacidad para el control de errores y el control de flujo con el fin de ahorrar procesamiento, dado que transmite a través de enlaces altamente fiables.
* Transferencia de paquetes con tamaño fijo, que se denominan celdas.
* Protocolo orientado a la conexión entre estaciones, con un ancho de banda a demanda en cada conexión. Con una trasmisión de celdas asíncronas, y con retardo fijo y pequeño.

**Celda ATM:**

Las celdas de tamaño fijo (53 bytes) se transportan sobre canales sincrónicos. Las celdas NO están sincronizadas respecto a ningún usuario, y las posiciones en el flujo se asignan por demanda.

|  |  |
| --- | --- |
| Encabezamiento | Información |
| 5 bytes | 48 bytes |

* Encabezamiento: Información de enrutamiento + prioridad, identificación de celdas de un mismo camino.
* Información: Transparente de extremo a extremo (datos voz o video).

**Encabezamiento de celda:**

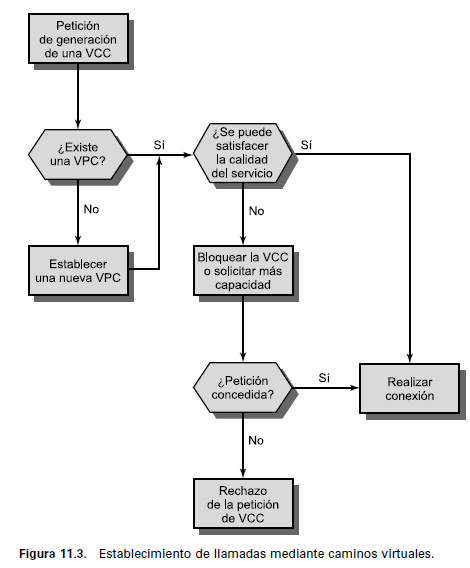
Existen dos tipos de celdas, una para interfaz red-usuario (UNI) y otra para celdas internas de la red (NNI).

|  |  |
| --- | --- |
|  |  |

* GFC: Control de flujo genérico.
* **VPI – Identificador de ruta virtual**: Utilizado para el enrutamiento dentro de la red.
* **VCI - Identificador de canal virtual:** Utilizado para el ruteo “ent-to-end”. Para encaminar hacia/desde el usuario final.
* PT (Payload type) - **Tipo de carga**: Identificador de tipo de información
  + 1er bit: Identifica el tipo de carga en el campo de Información.
  + **2do bit: Indica si hay error o congestión**.
  + 3er bit: Un 1 identifica extremo a extremo.
* **CLP (Cell Loss Priority)- Probabilidad de pérdida de celda.**
  + CLP = 0 => Tráficos asegurado y poco probable que se caiga o congestione.
  + **CLP = 1** => Tráficos de mejor esfuerzo. **La celda se puede descartar en caso de congestión**.
* **HEC - Control de errores en la cabecera**. Permite detectar errores y corregir hasta 1 de ellos. Para cada celda recibida se calcula y compara el HEC. Si no se detectan errores, el receptor permanece en el modo de **Corrección de Errores**. En cambio, si se detecta un error, el receptor lo corrige si se trata de un error simple o, en caso contrario, detectará la ocurrencia de un error múltiple. En cualquier caso, el receptor pasa a modo de **Detección**, no tratando de corregir errores

**Las conexiones lógicas en ATM son: [Ruta incluye a Canal]**

* **Conexiones de Canal Virtual (VCC):** Es la unidad básica de conmutación en ATM. Ésta se establece de tres maneras:
  + Usuario-usuario: Transportar los datos de extremo a extremo.
  + Usuario-red: Transportar órdenes a la red.
  + Red-red: Transportar datos de ruteo.
* **Conexión de Ruta virtuales (VPC)**: Conformada por un conjunto de Canales Virtuales (VCC) con los mismos extremos, conformado los caminos virtuales, reduciendo los controles necesarios.

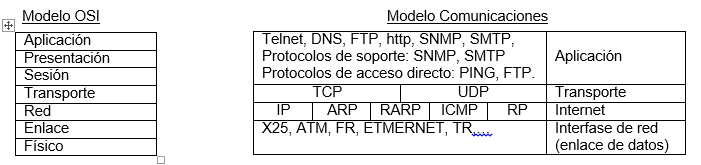


**Servicios ofrecidos por ATM:**

Una red ATM permite transmitir simultáneamente distintos tipos de tráfico con su formato de celda a través de un canal virtual, pero la forma en la que se trata cada uno de estos depende del flujo enviado.

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
|  | **CLASE A – ALL1** | **CLASE B – ALL2** | **CLASE C – AAL 3/4** | **CLASE D – AAL 5** |
| **Orientada a la Conexión** | SI | | | NO |
| **Sincronización (O-D)** | Requerida | | NO Requerida | |
| **Tasa Bit** | Constante | Variable | | |
| **Utilización / Servicios** | Audio y video SIN comprimir | Audio y video COMPRIMIDO | Datos | Datos |

# Capa Red / Internet (2 de 4) - IP | ARP | RARP | ICMP



**TCP-IP:** es un resultado de la investigación en la red ARPANET.

1. **Capa física**: Define la interfaz física entre el dispositivo de Tx y el medio de transmisión
2. **Capa de acceso a la red**: Es responsable del intercambio de datos entre el sistema final y la red a la cual está conectado. El emisor debe proporcionar dirección de destino, para que los datos puedan ser encaminados.
3. **Capa Internet**: Se encarga del encaminamiento de los datos a través de la red, establece una serie de procedimientos para que los datos atraviesen las distintas redes. Se utiliza el protocolo IP para este fin.
4. **Transporte**: es encargada de que los datos se envíen de forma segura y en el orden correcto de extremo a extremo, utiliza protocolo TCP.
5. **Aplicación**: Contiene la lógica necesaria para posibilitar las comunicaciones entre distintas aplicaciones de usuario en distintos computadores.

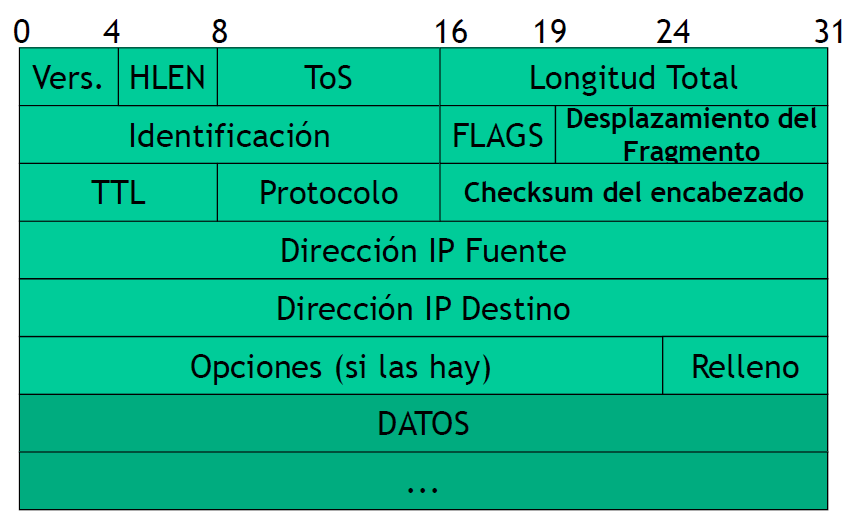
**Características**

* Para tener éxito en la transmisión cada entidad en el sistema global debe poseer dos direcciones: Dirección IP + Puerto.
* Para el funcionamiento, cada capa le envía la PDU correspondiente a la inferior (cada capa tiene su propia PDU), y finalmente esas PDU serán leídas en el otro extremo por las distintas capas.
* Usa ICMP para reportar errores.
* Se basa en servicio no orientado a la conexión (adaptable a las redes) y no confiable (pueden perderse, duplicarse, desordenarse, demorarse).
* Es un servicio de entrega con el mejor esfuerzo (best effort).
* Los datagramas enviados son independientes, no hay relación entre ellos. Estos pueden viajar por distintos tipos de redes (Connectionless).
* En vez de limitar el datagrama a un tamaño máximo, IP puede tratar la fragmentación y el re-ensamblado de sus datagramas. En particular, IP no impone un tamaño máximo, pero establece que todas las redes deberían ser capaces de manejar al menos 576 bytes.

## Datagrama IP

Protocolos de la capa de aplicación de TCP/IP:

* SMTP: Función básica de correo electrónico, proporciona un mecanismo para transferir mensajes entre computadores remotos.
* FTP: se utiliza para enviar ficheros de un sistema a otro bajo control del usuario.
* TELNET: Permite la conexión remota, con este esquema un usuario puede conectarse a un terminal remoto y manejarlo como si este fuera local.



**Campos**:

* Versión: versión del protocolo, actualmente existen IPV4 e IPV6
* HLEN: longitud de la cabecera expresada en palabras de 32 bits.
* Tipo de Servicio - ToS: parámetros de fiabilidad, prioridad, retardo y rendimiento.
* Longitud Total: del datagrama en octetos. Incluye la cabeceara (16 bits => Tamaño máximo de un datagrama 65.536 bytes)
* Identificador: número de secuencia que junto a las direcciones de origen y destino y el protocolo de usuario identifican unívocamente a un datagrama.
* FLAGS: sirven para el control de fragmentación.
  + el bit 0 está reservado y siempre debe ser 0
  + **el bit 1 “DF” significa NO fragmentar**: Si es 0 se permite la fragmentación y si es 1 se prohíbe la fragmentación.
  + **el bit 2 “MF” significa HAY más fragmentos**: Si es 0 se trata del último fragmento, y si es 1 significa que hay más fragmentos.
* Desplazamiento: indica el lugar donde se sitúa el fragmento con respecto al datagrama original.
* **Tiempo de vida (TTL): especifica el tiempo (en segundos) o cantidad de saltos que se le permite viajar al datagrama.** Sirve para determinar cuanta vida le queda al datagrama, si el contador llega a 0 se asume que el datagrama ha estado viajando en bucle y se desecha.
* Protocolo: identifica al protocolo de la capa superior cuya PDU residirá en el campo de datos. => ICMP = 1 |TCP=6 | UDP =11 o 17
* CheckSum: código de detección de errores aplicado sólo a la cabecera del datagrama.
* Fuente y Destino: Direcciones IP origen y destino, respectivamente.
* Datos: longitud múltiplo de 8 bits, el máximo es 64 KB.

**Direccionamiento IP**

* Emplean 32bits (4B), se representa en binario o con 4 decimales puntuados.
* Compuestos de: Identificador de clase + Identificador de red + Identificador de host.
* La dirección de cada red debe ser única y la de host debe ser única dentro de la red.
  + Si todos los bits de red son ‘1’ entonces estamos ante una máscara de red.

### Clases de Dirección:

* Clase A: **El primer bit del primer octeto siempre se estable en 0 (cero).**
* 8 bits red + 24 bits host => Las redes tienen un rango de 1 a 127
* Dirección Menor = 0.0.0.0 | Con 1er octeto =  **00000000**
* Dirección Mayor = 127.255.255.255 | Con 1er octeto =  **011111111**
* Máscara predeterminada = 255.0.0.0
* Cantidad de Redes = 2^7
* Cantidad de Host = 2^24-2 (ya que el o y el 127 están reservados)
* Clase B: **Los dos primeros bits del primer octeto siempre se estable en 10 (diez).**
* 16 bits red + 16 bits host => 128 a 191
* Dirección Menor = **128.0**.0.0 – Con 1er octeto =  **10000000**
* Dirección Mayor = **191.255**.0.0 – Con 1er octeto =  **10111111**
* Máscara predeterminada = 255.255.0.0
* Cantidad de Redes = 2^14
* Cantidad de Host = 2^16-2
* Clase C: **Los tres primeros bits del primer octeto siempre se establece en 110 (diez).**
* 24 bits red + 8 bits host => 192 a 223
* Dirección Menor = **192.0.0**.0 | Con 1er octeto =  **11000000**
* Dirección Mayor = **223.255.255**.0 | Con 1er octeto = **11011111**
* Máscara predeterminada = 255.255.0.0
* Cantidad de Redes = 2^21
* Cantidad de Host = 2^8-2
* Clase D
* 224 a 239
* Dirección Menor = 224.0.0.0 | Dirección Mayor = 239.255.255.255
* Su dirección comienza con 1110
* Clase E
* 240 a 247
* Dirección Menor = 224.0.0.0 | Dirección Mayor = 247.255.255.255
* Su dirección comienza con 1110

Direcciones Privadas:

* Clase A: 10.0.0.0 – 10.255.255.255
* Clase B: 172.16.0.0 – 172.31.255.255
* Clase C: 192.168.0.0 – 192.168.255.255

Tips:

* Una dirección de red no puede ser 127 porque esta reservada.
* Una dirección de red no puede ser 255 porque esta reservada para difusión.
* Una dirección de host con todos bits en 1 corresponde a difusión (Broadcast).
* Una dirección de host no puede ser 0 porque esa dirección es de red.
* Número de subredes = 2bits de subred – 2 (OJO: preguntar en el final si eliminamos las 2)
* Número de nodos por subred = 2bits host – 2

### Mensajes

* **Destino inalcanzable**: es enviado por el…
  1. Router - Cuándo no encuentra una red destino,
  2. Router - Cuándo declara que un host destino es inalcanzable,
  3. Router - Cuándo desea fragmentar un datagrama pero el bit de “NO fragmentar” está en 1.
  4. Host destino - Si se declara inalcanzable. Puede ocurrir si la cabecera de IP no tiene el valor correcto. Si el datagrama especifica una ruta destino que no se puede utilizar.
* **Tiempo excedido**: es enviado por el…
  + Router - Si el valor TTL del datagrama expiró (llego a 0);
  + Host – Si NO puede completar el reensamblado dentro del tiempo disponible.
* **Problema de parámetro**: Cuándo un error sintáctico o semántico en la cabecera de IP, lo envía un Router o un Host.
* **Ralentización del origen:** Puede enviarlo un Host Destino/Router solicitando que reduzcan la tasa de envío de información.
* **Redirección:** Lo envía un Router a un Host o Router para informar que existe una ruta alternativa mejor.

### Subred:

* Permite que una misma dirección de red identifique a varias redes físicas.
* Desde una red externa se va a ver todo como una gran red, pero internamente a cada LAN se le va a asignar un número de subred, el cual es tomado de la parte de HOST de la dirección IP. Para saber si dos direcciones IP corresponden a la misma subred basta con aplicarle un AND con la máscara de red, en caso de estar dentro de la misma subred, los paquetes no deberían pasar por un dispositivo de encaminamiento.
* Diseño de subredes necesitamos
  + Determinar Cantidad de Subredes + Cantidad de Host por cada Subred
  + Definir Mascara Subred + Dirección Subred + Rango de host válido por cada Subred

### Fragmentación y re-ensamblado

Como el tamaño de datagrama en distintas redes es variable, se utiliza la fragmentación. Consiste en dividir el datagrama en partes (más pequeños) que puedan encapsularse en MTU más pequeños, que luego se ensamblan en Destino.

* Basándose en el valor MTU, el campo de datos se divide en partes múltiplos de 8 bytes (tabla del 8), exceptuando la última. Debe ser el más próximo al MTU del trayecto (X es un número par que cumple con X=8\*K o se puede dividir 3 veces en 2)
* Cada fragmento es un datagrama independiente. Con el mismo Identificador, Dirección Origen y Destino que el Datagrama Original.
* El FLAG “Más Fragmentos” = 0 si es el último o el único fragmento.
* El FLAG “No fragmentar” = 1 impide la fragmentación. En tal caso el datagrama se descarta y se genera un mensaje ICMP
* MTU: Maximum Transfer Unit: Cada tecnología de conmutación de paquetes, fija un límite máximo para la cantidad de datos que pueden transmitirse en una única trama.

|  |  |
| --- | --- |
| **TECNOLOGÍA DE RED** | **MTU (Bytes)** |
| ETHERNET | 1500 => 1,5 Mb |
| DATAGRAMA IP | 65515=> 65,5 Mb |
| TOKEN BUS | 8182 => 8 Mb |
| TOKEN RING | 65535=> 65,5 Mb |
| X.25 | 128 (N3) |
| FRAME RELAY | 4090 => 4 Mb |
| ATM | 48 |
| FDDI | 4470 |

Desventajas: Duplicada la posibilidad de pérdida de un datagrama, genera mayor carga de procesamiento en los routers, y no es compatible con el Balanceo de Carga (Server farm)

### ESTRATEGIAS DE RUTEO / PROTOCOLO DE RUTEO / ENRUTAMIENTO / ENCAMINAMIENTO

Proceso que ocurre en la capa 3 – Red (Modelo OSI).

Para enviar un datagrama al siguiente host, un Router debe realizar dos funciones:

* Determinar el mejor camino a destino: revisa en las tablas de ruteo los caminos disponibles en la red y elige el óptimo.
* Conmutar el datagrama: cambiar la dirección física del datagrama por la del próximo salto.

*Objetivos de diseño de un protocolo de enrutamiento:*

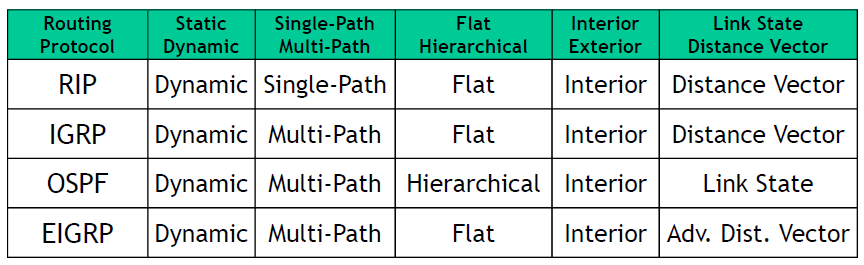
* *Flexible: Rápida adaptación a los cambios en la topología de la red.*
* *Óptimo: Elegir la mejor ruta de acuerdo con su métrica.*
* *Rápida convergencia: Permite que las tablas de ruteo estén consistentes/actualizadas, lo que impide un routing loops. Cuando ocurre un evento todos los Routers deben recalcular sus tablas.*
* *Robustez: Funcionar correctamente, aún en situaciones inusuales o impredecibles (ej. cogestión de los vínculos).*

**Métricas** para elegir la mejor ruta:

1. Cantidad de saltos.
2. Cantidad de saltos + Retardo de la red

**Clasificación** de los protocolos

* **Por vector distancia** (Distance vector): Los nodos mantienen un Vector de Costo por enlace para cada red conectada directamente. Intercambio de información con nodos vecinos.
* **Por estado de enlace** (Link state): Los nodos tienen la configuración completa de la red. Intercambian la información con todos los nodos de la red.



**Protocolo de Encaminador Interior (RIP)**

* Cálculo de métrica: Cantidad de saltos (valor Max. 15). Superada la cantidad máxima se declara “Host Inalcanzable”.
* Tipo: Vector Distancia (intercambio de información con vecinos).
* Ventajas: Confiabilidad - Transmisión periódica de las tablas. La v2 incluye la información de las subredes en la tabla.
* Mensajes: Encapsulado en datagramas UDP (puerto 520).
  + Cada 30 seg: encapsula el contenido de la tabla de ruteo y lo envía a todas las interfaces.
  + Cada 120 seg: retira las rutas con métrica infinita.
  + Cada 180 seg: si una ruta no fue actualizada, se le setea su métrica en infinito y se informa a los vecinos.
* Problema: generar un agujero negro poniendo una ruta con mayor calificación + fácil de quebrar su seguridad

**Protocolo Primer Camino Más corto Disponible (OSPF)**

* Cálculo de métrica: Ancho de banda de referencia / Ancho de banda de la interfaz.
* Tipo: Estado de Enlace (intercambio de información con todos los routers de la red).
* Ventajas:
  + Converge más rápido e intercambia menos información que RIP. Se usa en redes TCP/IP.
  + Permite el balanceo de cargas (enviar por 2 caminos). Seguridad es robusta, y acepta subredes.
* Mensajes: Encapsulado sobre IP, protocolo 89.
  + Solo envía las actualizaciones de tabla.

## Protocolos ARP – RARP (para resolución de direcciones):

* **ARP**: Permite conocer la dirección MAC a través de su dirección IP. Transmite una difusión (Broadcast) con la IP destino al servidor ARP y este le responde con la MAC destino.
  + *ARP Request: Es un Broadcast preguntado a todos quién tiene X dirección IP.*
  + *ARP Reply: Es un Unicast, enviado desde el host destino buscado al host origen que preguntó.*
  + ***ARP Gratuito****: Un Host pregunta quién tienen su dirección IP. Sirven para:*
    - *Evitar la activación repetida de una misma IP => Detectar conflictos de IP*
    - *Actualizar el contenido de la cache ARP*
    - *Informar a los switch la dirección MAC del host que envía el msj.*
* **RARP**: Permite que una máquina conozca su dirección IP a través de la MAC. Transmite en difusión (Broadcast) MAC al servidor RARP y este le devuelve la IP de la máquina.

|  |  |
| --- | --- |
|  |  |

## Protocolo IGMP – Protocolo de Gestión de Grupos de Internet

Utilizado para consultar e informar el estado de pertenencia al grupo de multidifusión de una red LAN.

Los mensajes IGMP se transmiten en datagramas IP. Existen dos tipos de mensajes:

* Routers – Consultan a los Host la pertenencia a grupo de multidifusión.
* Hosts – Informan a los Routers la pertenencia a grupo de multidifusión.

## Protocolo ICMP - Detección de errores

Surge con la idea de solucionar los problemas de IP. Comunica Errores a nivel de red e Informa acerca de eventos inesperados. Solo informa el error, no especifica que acción correctiva tomar

Los mensajes son dos tipos:

* **Reporte de error:** 
  + **Destino inalcanzable**: Ante la imposibilidad de conmutar/entregar un datagrama el Router envía un mensaje ICMP antes de descartarlo.
  + **Tiempo de espera** agotado: Cuándo TTL se decrementa y llega a 0 + Cuándo el host desiste de esperar un fragmento.
* **Consulta/Respuesta:** 
  + **Echo request/reply**: Utilizado para conocer si la interfaz destino es alcanzable y está funcionando (PING).

**Comando**

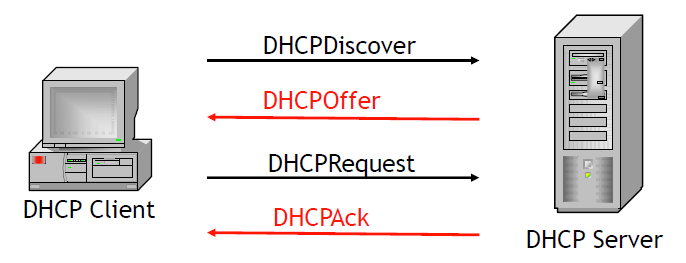
* **PING:** Es un mensaje de tipo ICMP. Se utiliza para analizar la conectividad de un dispositivo de red (si puedo llegar a él), para saber cuánto tiempo tardan en ir y volver los datos y a que velocidad de transmiten. Consiste en enviar un eco request al destino y esperar un respuesta.
* **TRACEROUTE**: Es un mensaje de tipo UDP. Se utiliza para descubrir la ruta que recorre un mensaje hasta llegar al destino. Consiste en enviar datagramas con TTL=1 + N (según la iteración) a cada router en el camino, estos responderan con un mensaje ICMP de Tiempo Excedido (TEM)

## Protocolo DHCP – Dynamic Host Configuration Protocol

Centraliza y administra la asignación de direcciones IP. Manteniendo un inventario de direcciones IP asignadas.

Tipos:

* Asignación estática.
* Asignación Dinámica: Elimina la necesidad del inventario, facilita la modificación del espacio de direcciones, elimina la existencia de errores.



*Funcionamiento*

1. *DHCP Discover: El cliente envía un pedido de dirección IP a los servidores DHCP*
2. *DHCP Offer:Los DHCP Server que reciben la consulta responden:*
   1. *Dirección de hardware del cliente*
   2. *Dirección IP destino 0.0.0.0*
   3. *Una dirección IP ofrecida => La reserva.*
   4. *La máscara de subred*
   5. *Duración de la asignación (Lease)*
   6. *Una identificación del servidor (dirección IP)*
3. *DHCP Request: el cliente envía un broadcast a todos los Servers indicando la oferta aceptada.*
4. *DHCP ACK: El DHCP Server cuya oferta fue aceptada, envía una confirmación positiva al cliente con la dirección IP asignada. NACK es una respuesta negativa.*

*Otros mensajes:*

* *DHCPDecline – El cliente indica al servidor que la dirección está en uso. (Gratuitous ARP)*
* *DHCPRelease – El cliente libera la asignación, cancelando el lease*
* *DHCPInform – El cliente solicita sólo los parametros de configuración adicionales*

# Capa Transporte (3 de 4) TCP – UDP

El protocolo de transporte proporciona un servicio de transferencia de datos punto a punto que aísla las capas superiores de los detalles de la red.

Un protocolo de transporte puede ser:

* Orientado a conexión: TCP
* NO orientado a conexión: UDP.

## TCP – Transmission Control Protocol

La combinación de una dirección IP y puerto usado se denomina Socket, una comunicación TCP es identificada completamente por las direcciones de los sockets en los extremos.

**A) Conexión: Orientado a la conexión**

Consta de 3 pasos.

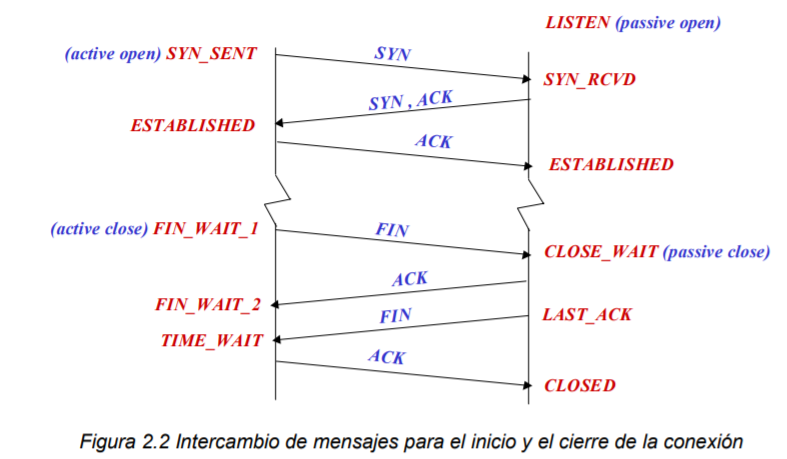
1. **Establecimiento de la conexión:** el emisor manda un mensaje de establecimiento de conexión, el receptor devuelve un mensaje de aceptación y el emisor comienza el envío.
   1. Iniciador envía un mensaje SYN-1 + Número de Secuencia-X.
   2. En caso de aceptar, Receptor responde con un mensaje SYN-1 + Número de secuencia-Y + Acuse de recibo ACK-(X+1).
   3. iniciador recibe y responde con un mensaje ACK-(Y+1).
2. **Transferencia de datos**: empieza el período de intercambio de datos hasta que el programa de aplicación informa a TCP que ya no tiene más datos para enviar.
3. **Cierre de la conexión: 4 pasos**

1. El cliente envía un segmento solicitando el cierre de conexión, éste no tiene datos solo la bandera FIN.

2. El servidor responde con un segmento ACK, confirmando la recepción del FIN. A partir de éste momento, el Cliente ya no puede enviar mas datos (cierre de conexión en 1 sentido).

3. El servidor envía un segmento solicitando el cierre de conexión, éste no tiene datos solo la bandera FIN.

4. EL cliente confirma la recepción del FIN mediante el envío de un ACK (conexión cerrada en 2 sentidos).



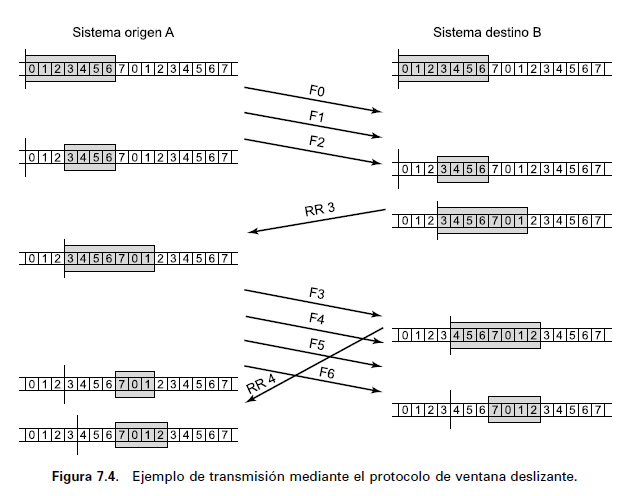
**B) Sentido de la Conexión: Full – duplex**

Puede enviar y recibir paquetes al mismo tiempo.

**C) Transferencia de datos: FIABLE** mediante **el control de flujo “Ventana Deslizante”**

Es de tipo “**Stop and Wait**”. Por lo tanto, cada trama enviada debe tener una confirmación.

* Consiste en enviar múltiples tramas, sin importar que tenga una confirmación, y luego esperar la confirmación de cada una de ellas.
* Claves: Las tramas poseen un número de secuencia para mantener el orden + Se define una ventana de tamaño fijo (buffer) + necesitamos las confirmaciones (ACK) para continuar enviando tramas.
* Tenemos 2 tipos de ventanas:
  + Ventana de recepción: cuántos bytes se pueden recibir.
  + Venta de emisión: cuántos bytes se pueden transmitir sin tener que esperar un ACK.
  + Debe definirse cuántos segmentos pueden enviarse, para ello se calcula: ANWD = Min [cnwd, credit]
    - **ANWD: Cantidad de segmentos** que puedo enviar ahora, sin esperar ACK.
    - **CNWD: Ventana de congestión**, al momento 0 no posee valor.
    - **CREDIT: Bytes permitidos por el destino**.



* + F-X => A trasmite la trama X a B
  + RR-Z => B confirma que recibió correctamente hasta la traman Z-1 y espera recibir la trama Z.
  + RNR Y =>B confirma que recibió correctamente hasta la trama Y, y prohíbe la trasmisión de más tramas.

**D) Transferencia de datos- Control de Congestión**

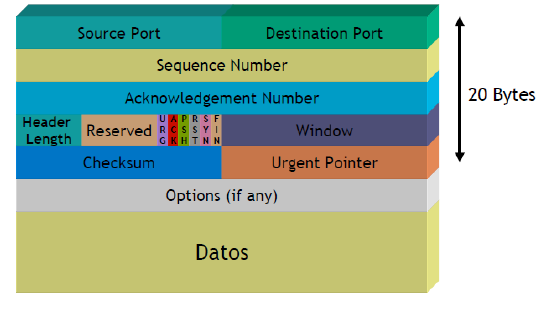
* + **Slow Start:** Cada vez que se recibe una confirmación ACK se incrementa en 1 el valor de Ventana de Congestión (CNWD), que determina cuánto segmentos puedo enviar sin esperar un ACK. Cuando un segmento se pierde o caduca el RTO, el valor de CNWD = 1 (como al inicio).
  + **Fast Recovery**: Cuando se recibe el 3er ACK duplicado, se setea CWND = CWND / 2
  + **Fast Retransmit**: No resulta apropiado precipitar la retransmisión ante la recepción del 1er ni el 2do AK duplicado. Entonces, solo si se reciben 3 ACK, se retransmite el segmento perdido.

**E) Transferencia de Datos: CONFIABLE, mediante la identificación y el control de errores.**

Se realiza con la ayuda de lo siguientes campos:

* **Número** de secuencia: Necesario para ordenar los paquetes, detectar aquellos perdidos y eliminar duplicados.
* **Suma de Comprobación (**Checksums**)**: Necesario para detectar errores, pérdidas y retrasos.
* Utiliza time-out para retransmisión. Transferencia confiable de extremo a extremo.
* No existe una confirmación de rechazo, ésta se supone si por un tiempo predeterminado (RTO) no ha llegado el ACK, y en tal caso se retransmite. RTO es el temporizador de retransmisión (también conocido como el valor de expiración de retransmisión). debe ser suficientemente pequeño como para responder rápidamente a las pérdidas, pero no tanto como para forzar la retransmisión de datos que han sufrido un pico de retardo en la red sin haber llegado a perderse.

**F) Datagrama**



## UDP – User Datagram Protocol

**A) Conexión: NO orientado a la conexión**

Por lo tanto, no mantiene un estado de conexión.

**B) Sentido de la Conexión: Single – Duplex**

Puede enviar o recibir, pero solo una cosa a la vez.

**C) Transferencia de datos: NO es fiable**, no posee un c**ontrol de flujo.**

Por lo tanto, no puede garantizar que un paquete se recibido (o no) y el orden de este.

No envía notificación de recepción (ACK).

**E) Transferencia de Datos: NO es fiable, si bien identifica errores NO puede corregirlos**

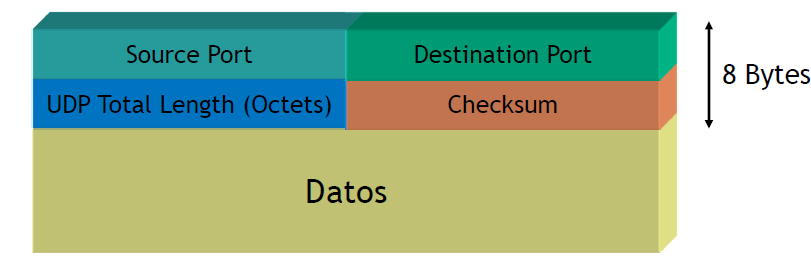
Al no tener corrección de errores, no posee un Control de Congestión.

Al recibir un datagrama, si y hay lugar en el buffer, lo encola. Si no hay lugar, lo descarta. No envía mensaje de error.

Suma de Comprobación (Checksums): Al detectar paquetes erróneos, simplemente los descartan.

**F) Datagrama**

Es útil para: Streaming de audio y video



# Capa Aplicaciones (4 de 4) - DNS/

## Aplicaciones: 1- Protocolo DNS – Domain Name System

Es un sistema de nomenclatura jerárquica para los dispositivos conectados a Internet o a una red privada.

Su función más importante, es traducir nombres de Host en direcciones IP, esto con el propósito de poder localizar y direccionar estos equipos mundialmente.

* Protocolos y puertos: 53 para UDP y TCP.
* Está compuesto por varios niveles de dominio para resolver la jerarquía de nomenclaturas.
* Poseen limitadas Zonas de implicancia, para la cual cada servidor DNS es responsable.

Tipos de consultas

* **Consulta Recursiva**: El servidor de nombres consultado está obligado a responder con los datos o con un error
* **Consulta Iterativa**: El servidor consultado responde con su mejor respuesta (el nombre resuelto o una referencia a otro servidor de nombres).
* **Consulta Inversa**: Determina el Nombre de Host asociado a una IP dada.

## Aplicaciones: 3- FTP

Transferencia de archivos.

Capa Aplicación del Modelo TCP/IP | **Puerto** 20 y 21

*PD: SFTP está en el puerto 69, y es mucho más simple. Cumple el mismo objetivo, la transferencia de archivos.*

## Aplicaciones: 4- SFTP

Transferencia de archivos que utiliza SSH para asegurar los comandos y datos transferidos (autenticación y encriptación)

Capa Aplicación del Modelo TCP/IP | **Puerto** 22

## Aplicaciones: 5 – Telnet

Utilizado para la administración remota de los dispositivos de red.

Capa Aplicación del Modelo TCP/IP. | **Puerto 23**

## Aplicaciones: 6 – SMTP

Protocolo simple de transferencia de correo electrónico, mediante una conexión punto a punto, directamente al servidor destino.

Capa Aplicación del Modelo TCP/IP. | Puerto 25

## Aplicaciones: 7- HTTP

Transferencia de (petición/envió) de Hipertexto. Se basa en operaciones de Solicitud/Respuesta.

Capa Aplicación del Modelo TCP/IP | **Puerto** 80

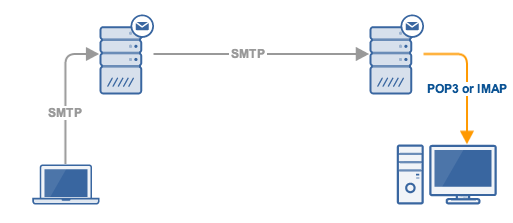
## Aplicaciones: 8- POP o IMAP

Envió y recepción de correos electrónicos **desde el servidor al cliente.**

**POP**: Permite descargar los correos y los elimina del servidor (salvo configuración contraria), éstos pueden ser vistos sin una conexión a internet. Los cambios realizados a nivel aplicación local, no se sincronizan con el servidor.

**IMAP**: Accede directamente al servidor, nunca descarga los correos / Sincronización on-line.

**Puertos**: POP – 110 | IMAP - 143



## Aplicaciones: 9 – SNMP

Permite la administración de red.

Capa Aplicación del Modelo TCP/IP. | Puerto 161

# Seguridad

La seguridad implica los siguientes requisitos (CIDA):

* ***Confidencialidad***: sólo las personas autorizadas pueden tener acceso a los datos
* ***Integridad***: los datos solamente pueden ser modificados por partes autorizadas.
* ***Disponibilidad***: los datos estén disponibles para las partes autorizadas.
* ***Autenticidad***: poder establecer la identidad del emisor y el receptor.

**Clases de ataques:**

* ***Pasivos***: Captura de datos sin afectar o interferir en los sistemas, consisten en escuchas o monitorización de las transmisiones, el objetivo puede ser hacer un análisis del tráfico o divulgar un contenido determinado.
* ***Activos***: Captura de datos que supone una modificación del flujo de datos o la creación de flujos falsos.
  + *Enmascaramiento*: cuando una entidad simula ser otra para hacerse de datos, etc.
  + *Retransmisión*: supone la captura de datos y su retransmisión para producir un efecto.
  + *Modificación de mensajes*: un mensaje legítimo se modifica para producir un efecto no autorizado.
  + *Denegación de servicio*: impide el uso normal o gestión del servicio de comunicaciones.

**Cifrado simétrico - *Encriptación con clave privada***.

Garantiza la integridad y confidencialidad

* Texto nativo: mensaje original o datos de entrada.
* Algoritmo de cifrado: procesa una entrada de texto nativo en bloques de tamaño fijo y produce un bloque de texto cifrado de igual tamaño.
  + DES: Fue el primer algoritmo de cifrado que surgió, emplea claves de 56 bits. También existe 3DES, que supone la repetición del algoritmo DES básico 3 veces.
  + AES: Algoritmo más moderno que emplea clave de 128 bits.
* Clave privada: la clave secreta es una entrada del algoritmo de cifrado, este depende de ella para generar una salida determinada.
* Texto cifrado: es el mensaje nativo alterado por el algoritmo de cifrado.
* Algoritmo de descifrado: el algoritmo de cifrado ejecutado a la inversa.

***Cifrado asimétrico – Encriptación con clave privada y pública***

Garantiza la integridad, confidencialidad, autenticidad y No-repudio. Se basa en el uso de dos llaves para poder cifrar y descifrar, los componentes son:

* *Texto nativo*
* *Algoritmo de cifrado.*
* *Clave pública y privada*: es un par de claves que se seleccionan de tal modo que si una se usa para el cifrado, la otra se usa para el descifrado. Las transformaciones realizadas por el algoritmo de cifrado dependen de una de estas claves.
* *Texto cifrado*: producido como salida del algoritmo de cifrado.
* *Algoritmo de descifrado*: acepta el texto cifrado y la clave correspondiente, produciendo el texto original.

**Funciones HASH:** Toma una entrada, y genera una salida de longitud fija. Garantizan la integridad del mensaje.

* Consistencia: La misma entrada, siempre debe generar la misma salida.
* Unicidad: dos entradas diferentes no pueden nunca generar la misma salida.
* Aleatoriedad al generar el hash, que impida adivinar el mensaje de entrada.
* Un camino: desde la salida, nunca se debería poder reversar al mensaje de entrada.

**Firmas digitales:** es un código encriptado que se adiciona a un documento. Garantiza identidad e integridad.

Es un mecanismo que permite determinar con seguridad quien envió un mensaje, por ej. un A puede cifrar un mensaje con su clave privada y enviárselo a B, quien conoce su clave pública, luego B al poder descifrar el texto cifrado con la clave pública de A, se asegura de que este fue producido con la clave privada de A, por lo tanto, se asegura de que este fue quien envió el mensaje.

*Seguridad en OSI.*

La capa de sockets segura (SSL) junto con la capa de transporte segura (TLS) son ampliamente utilizados para dar seguridad. SSL es un servicio de propósito general implementado como un conjunto de protocolos que hacen uso de TCP. SSL puede disponerse de tal forma que sea subyacente a las capas existentes y transparentes a las aplicaciones o podría estar embebido dentro de las aplicaciones.

SSL hace uso de TCP para proporcionar un servicio fiable y seguro de extremo a extremo. El protocolo de registro SSL proporciona servicios básicos de seguridad a varios protocolos de capas superiores.

Existen dos conceptos importantes en SSL:

* *Conexión*: una conexión es un transporte que proporciona un servicio adecuado, son relaciones entre pares, son transitorias, cada una de estas se asocia a una sesión.
* *Sesión*: es una asociación entre un cliente y un servidor. Las sesiones son creadas por el protocolo de negociación bilateral, éstas definen un conjunto de parámetros de seguridad criptográficos, que pueden compartirse entre múltiples conexiones.

SSL ofrece dos servicios:

* *Privacidad*: el protocolo de negociación bilateral establece una clave secreta compartida que es utilizada para el cifrado simétrico de cargas útiles SSL.
* *Integridad del mensaje*: el protocolo de negociación bilateral también define una clave secreta que se utiliza para formar un código de autenticación de mensajes (MAC).

*Fases de SSL*:

* Negociar entre las partes el algoritmo que se usará en la comunicación (puede ser de clave pública RSA, o de cifrado simétrico AES, DES,3DES).
* Intercambio de claves públicas y autenticación basada en certificados digitales
* Cifrado del tráfico basado en cifrado simétrico