TEMA 3. PROTOCOLOS DE INTERCONEXIÓN DE REDES

EL PROTOCOLO DE INTERNET (IPv4)

OBJETIVO BÁSICO:

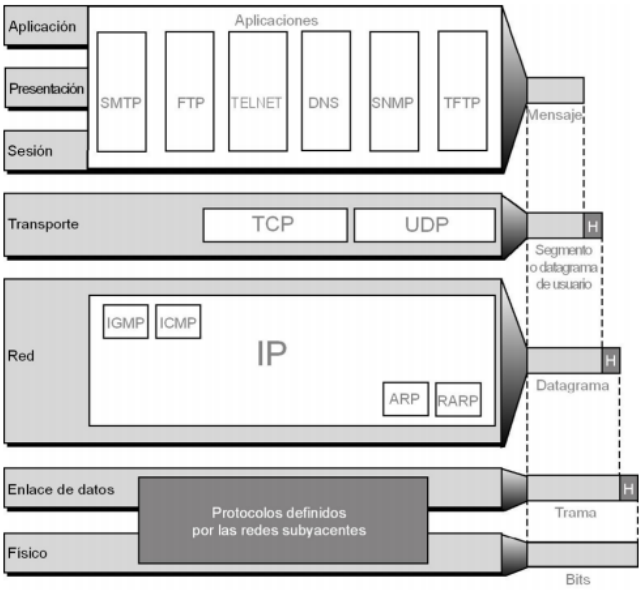
Enviar los paquetes del nodo emisor al nodo receptor a través de una red de conmutación de paquetes. Los nodos puedes no estar conectados directamente entre ellos.

Dado que puede haber varias rutas posibles, la capa de red es la encargada del encaminamiento.

EL PROTOCOLO IP:

Es el corazón de TCP/IP y es el protocolo más importante de la capa de red.

IP facilita el servicio de reparto básico de paquetes de las redes TCP/IP.



Se llama PDU (Protocol Data Unit) se utiliza para el intercambio de datos entre las distintas unidades.

ARP se encarga de traducir los datos entre el nivel de red, donde utilizamos IP, y el nivel de enlace que utilizamos MAC.

La imagen muestra las distintas capas con sus respectivos protocolos.

SERVICIOS QUE OFRECE IP:

- IP es un protocolo sin conexión. Es decir, no es necesario un intercambio previo de información antes del traspaso de datos para establecer una conexión.
  Deja en manos de las capas superiores el establecimiento de la conexión si se requiere.

- IP deja en manos de otras capas la verificación de datos y la recuperación de errores.
  - Detecta errores, pero no hace nada por recuperarse de ellos. Los routers descartan los paquetes.
  - Los protocolos de otras capas han de proporcionar control de errores si éste es requerido.
- Primitivas:
  - Enviar datos.
  - Recibir datos.

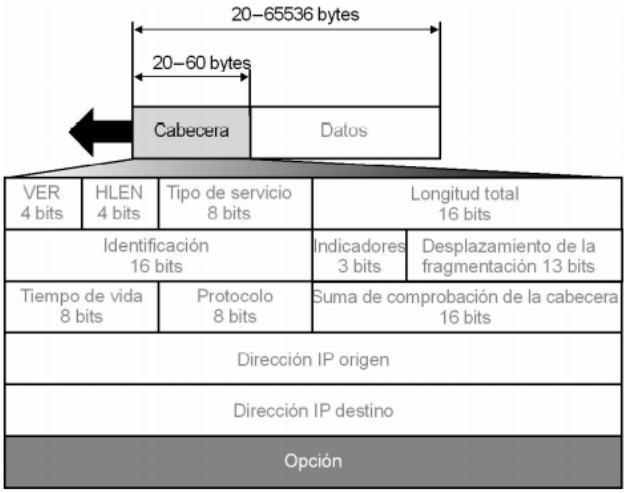
FUNCIONES DEL PROTOCOLO IP:

Las funciones básicas son:

- Definir el datagrama (también llamado paquetes o mensajes de nivel de red)
- Definir el esquema de direccionamiento
- Trasladar los datos entre las capas de acceso a la red y las capas de transporte.
- Encaminar datagramas a ordenadores remotos
- Fragmentación y reensamblado de datagramas (*se detallará más adelante*)
- Control de congestión: Descarte de paquetes

DATAGRAMAS IP:

Contiene una cabecera, con una parte fija de 20 bytes y una parte variable, y los datos.



VER: Indica la versión del protocolo (En IPv4 este campo contiene 0100 = 4).

HLEN: Longitud de la cabecera.

Tipo de servicio: Expresa la prioridad de los paquetes.

Longitud total: longitud del datagrama.

Identificación, Indicadores y desplazamiento de la fragmentación: Campos necesarios para la fragmentación y su posterior reensamblado.

Tiempo de vida: N.º de saltos que puede dar mi paquete en la red. Este número se decrementa cada vez que salta y cuando llega a 0 el paquete se descarta. Este es un mecanismo contra la congestión.

Protocolo: Indica a qué protocolo siguiente tengo que darle el contenido (cada protocolo tiene asociado un número que lo identifica).

Suma de comprobación de la cabecera (CHECKSUM): Suma a complemento a 1 de los campos que queramos, dividiéndolos en bloques de 16 bits y, a cuyo resultado se le aplica el complemento a 1.

DIRECCIONES IP:

- Las direcciones IPv4 son únicas y universales, de longitud 32 bits.
- Tres tipos de direcciones:
    - Unicast: Identifica a una sola máquina
    - Multicast: Representa a un conjunto de máquinas
    - Broadcast: Determina a todas las máquinas que están en redes locales. Si mando un mensaje a esta dirección IP, les llegará a todas las máquinas que se encuentren en mi red local.

DIRECCIONAMIENTO IP:

El encaminamiento en IP es un encaminamiento jerárquico:

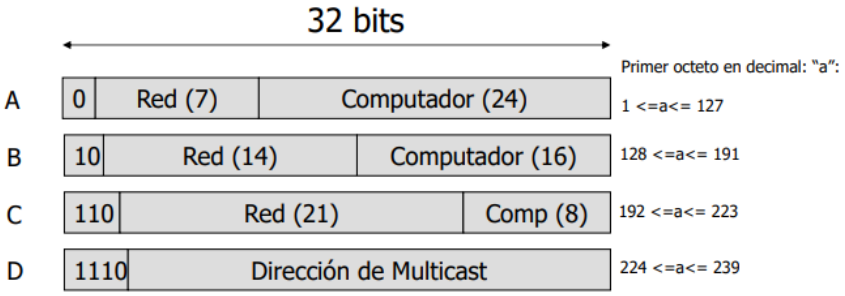
- En IP se realiza una jerarquía de encaminamientos de **dos niveles**, según la cual una dirección IP se divide en una parte para la **red** y otra para el **host** (dispositivo).

    - **<id.Red><id.host>**: El router, para decidir la salida por la que va a llevar el paquete hasta su destino solamente se fija en el identificador de red <id.Red>. Estos valores pueden cambiar a lo largo del camino.

- Los routers usan únicamente la parte de la red hasta que un datagrama IP llega a un router que puede entregar el paquete directamente.

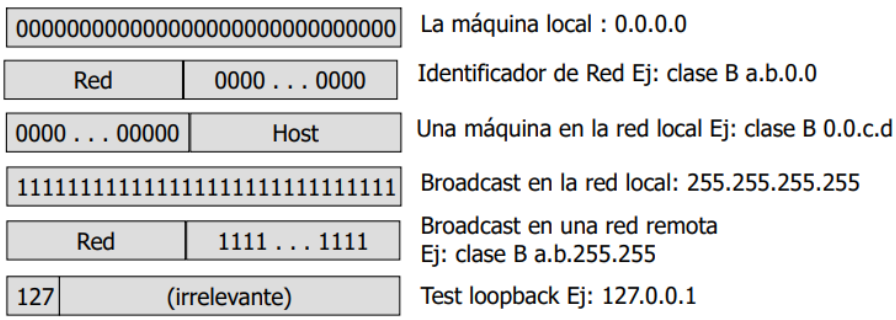
    - Únicamente el router que se encuentra conectado a la red dónde está la máquina a la que va a llegar el paquete, se fija en la dirección del host y manda una entrega directa a la máquina destino. Durante la vida del paquete en la red se van produciendo **dos tipos de entregas**:
        - **Entrega indirecta**: El router que se fija en el identificador de red realiza esta entrega. Esto se debe a que no puede entregar nada a la máquina destino y en su lugar, se lo da a otro router que se encuentra más cerca de la máquina final.
        - **Entrega directa**: Lo realiza el router que presenta una conexión de área local con la máquina destino, entregando directamente el paquete. Esto lo hace usando protocolos como ARP.

Formatos de direcciones IP:



- El espacio de direcciones se divide en 5 clases A, B, C, D y E (no se usa)

Direcciones IP especiales:



Loopback (Lo) representa una interfaz de red ficticia presente en todos los equipos, en la que todas las máquinas, independientemente de que tengan acceso a la red, pueden ejecutar aplicaciones de red, eliminando así la necesidad de programas dos tipos de aplicaciones (escritorio y red).

Es muy utilizada para realizar pruebas (tests) con aplicaciones de red.

NOTACIONES IP – REPRESENTACIÓN:

- **Binaria**: la dirección IP se muestra como 32 bits
  - **Ej**: 11111111111111111111111111100000
- **Notación Decimal – punto**: Se separan por puntos en 4 grupos de 8 bits. Cada grupo se representa en decimal (0-255).
  - **Ej**: 255.255.255.224, 111.56.045.78, 221.34.7.82, …

NAT (NETWORK ADDRESS TRANSLATION):

Es un mecanismo utilizado por routers IP para cambiar paquetes entre dos redes que asignan mutuamente direcciones incompatibles. Consiste en convertir, en tiempo real, las direcciones utilizadas en los paquetes transportados.

- Hacen uso de direcciones privadas (o locales)
- Se denominan redes privadas
- Son únicas dentro de una organización
- Ningún router reenvía al exterior un paquete con direcciones de origen privadas

SUBREDES:

Se trata de una división de una red muy grande que consiste en utilizar algunos bits pertenecientes a la dirección host con intención de identificar una subred dentro de una red. Eso se lleva a cabo mediante la ayuda de la máscara de red, que es una secuencia binaria en la que los 1's marcan aquellos bits que representan <id.Red> y los 0's representan <id.Host>

- **Ej:** *IPv4 = 192.168.1.136 y Máscara de red = 255.255.255.0*
  <id.Red><id.Subred> = 192.168.1 y <id.host> = 136

Si realizo una operación AND entre la dirección IP y la máscara, podré obtener la dirección de dónde se encuentra la máquina o, de forma más sencilla, poniendo los bits de <i.host> a 0.

Para determinar el número e identificador subred, me fijo qué número representa en decimal aquellos bits destinados a la subred. El <id.subred> será toda la IP menos el host.

En resumen:

- Se puede dividir un bloque de direcciones en varios grupos de direcciones más pequeñas.
- Se usan varios bits del identificador de host para constituir un identificador de subred
- Si tomo 'n' bits, entonces puedo definir 2n subredes
- Asignar cada grupo a redes más pequeñas -> subredes
- El tamaño de cada subred disminuye según el número de bits asignados para identificador de subred
- **Máscara de subred**:
  - Patrón de 0s y 1s para calcular el identificador de subred a la que pertenece un equipo

Ejemplo:

IPdestino: 192.228.17.57

	Representación Binaria	Representación Decimal
Dirección IP	11000000.11100100.00010001.00111001	192.228.17.57
Máscara de subred	11111111.11111111.11111111.11100000	255.255.255.224 (equivale a prefijo /27)
Operación AND de dirección y máscara	11000000.11100100.00010001.00100000	192.228.17.32
Número/Identificador de subred	11000000.11100100.00010001.00100000	1/192.228.17.0 (hay 8 posibles)
Número/identificador de máquina	00000000.00000000.00000000.00011001	25

FRAGMENTACIÓN Y REENSAMBLADO:

La fragmentación surge debido a que el tamaño del paquete a transmitir es mayor que el tamaño de la MTU (máxima cantidad de datos que se puede pasar en una trama) de mi máquina. Para ello, el paquete se fragmenta en varios sub-paquetes de tamaño menor o igual que la MTU y con cabecera propia.

Una vez ha pasado la MTU, se deben reensamblar o recomponer el datagrama original antes de entregarlo a la capa de transporte del host destino.

Existen algunos inconvenientes:

- Costoso de implementar computacionalmente.
- Coste que incide en el tiempo de entrega del datagrama original.

Campos de la cabecera relacionados con la fragmentación:

- **Identificador**: Es el mismo para todos los fragmentos. Necesario para poder reensamblarlos.

- **Indicadores**: Permiten conocer si un fragmento es el último de una secuencia de fragmentos o no con el flag M (more fragments) y si es posible realizar la fragmentación, para ello se utiliza el flag D (Do not fragment).

	D	M

- **Desplazamiento**: Comunica el orden de los fragmentos para su reensamblado. El desplazamiento de los fragmentos intermedios debe ser múltiplo de 8.

PROTOCOLOS ASOCIADOS A IP:

IP es de tipo *best-effort* y necesita de otros protocolos

Clasificación de los protocolos asociados a IP:

- **Protocolos de resolución de direcciones**: ARP, DHCP, etc.
- **Gestión de grupos (envíos multicast):** IGMP
- **Alertar de errores y monitorización de red:** ICMP
- **Actualización de tablas de encaminamiento:** RIP, OSPF

Protocolos de resolución de direcciones – ARP

La entrega de un paquete requiere el uso de una dirección lógica y de una dirección física. Por tanto, debemos ser capaces de traducir una dirección lógica a su correspondiente dirección física y viceversa.

Es decir, permite traducir direcciones IP a direcciones de nivel dos o hardware y, al contrario. Además, indica cuál es la dirección de nivel de enlace que está asociada a una dirección IP concreta. Esto lo hace preguntando a todas las máquinas (por una petición mediante broadcast) qué máquina tiene la dirección IP que necesita y la que lo tenga, envía un mensaje.

Para no tener que estar realizando esta operación en todo momento, ARP dispone de una caché que almacena de forma temporal la IP de una máquina tras una petición y su correspondiente respuesta y antes de enviar una petición, consulta la caché. No obstante, esta información no la guarda de forma permanente, debido a que las direcciones IP pueden cambiar.

Existen cuatro casos de uso de ARP:

- **Entrega directa**. Si tengo una máquina y quiero enviar un mensaje a una que está en mi misma red, lanzaré un mensaje saber cuál es la máquina que está dentro de mi misma red.
- **Entrega indirecta**. En este caso, la máquina tiene que averiguar la IP del router al cual tengo que enviarle el paquete.
- **Dos router están usando una red para enviar un paquete cuyo destino no está en esa red**. En este caso, un router hace una llamada ARP para averiguar la IP del otro router.
- **En el caso de una entrega directa entre un router y una máquina**, el router será el que utilice una llamada ARP para averiguar el IP de destino.

Protocolos de resolución de direcciones – DHCP

Es un protocolo que permite asignar una dirección IP a una máquina de manera automática para ser usada dentro de esa red.

Los mecanismos para asociar IPs son:

- **Asignación manual**. Puedo asociar a una interfaz la misma IP.
- **Asignación automática**. Asigna una IP permanente cuando se solicita.
- **Asignación dinámica**. Concede una IP temporalmente cuando se solicita.

Funcionamiento básico:

Cuando llega la máquina a la red manda un mensaje de descubrimiento ya que no tiene IP (dirección de origen 0.0.0.0) y lo manda a broadcast (255.255.255.255) pidiendo una dirección IP.

El servidor DHCP recibe la petición y le envía otro mensaje a broadcast con una oferta de dirección IP que le llega a la máquina que realizó la petición.

Esta máquina, tras recibir la oferta, vuelve a mandar una petición formal y el servidor DHCP le confirma. La confirmación lleva la IP que se le ha otorgado como dirección destino.

Cuando tenemos más de un servidor DHCP en la misma red:

El cliente manda el mensaje de descubrimiento que llega a los servidores DHCP, los cuales envían una oferta a la máquina. En el caso de que le llegue solo una, realiza toda la operación con ese servidor. En otro caso, manda tantas peticiones como servidores DHCP haya en la red, pero solo en una de ellas va a indicar que continúe con la operación y el resto abortarán.

Cuando pasa cierto tiempo hay que liberar la IP, por ejemplo, cuando una máquina se va a desconectar de la red o cuando va a finalizar el tiempo que le ha sido otorgado. Para ello, establezco un temporizador.

Otro caso en el que dispongo de un temporizador es cuando se va a pedir una renovación del tiempo otorgado o cuando deseo cambiar la configuración.

Protocolos de gestión grupos multienvío:

Debido al tipo de direccionamiento, IP está involucrado en tres tipos de comunicación: UNICAST (dirección individual), BROADCAST (dirección difusión) y MULTICAST (dirección de grupo – clase D).

El protocolo de red IGMP (Internet Group Management Protocol) o Protocolo de gestión de grupos en Internet se utiliza para intercambiar información acerca del estado de pertenencia y encaminamiento a un grupo multicast.

IGMP define un par de mensajes: unión a un grupo o abandono de un grupo. Además de mensajes de monitorización de pertenencia.

PROTOCOLO DE CONTROL Y NOTIFICACIÓN DE ERRORES – ICMP

ICMP es un protocolo que sirve de apoyo a IPv4. Además, el comando ping utiliza este protocolo.

Protocolo de control de mensajes de Internet

- Mensajes de monitorización y de informes de error

Mensajes de informe de error

- Informan y no corrigen errores que un dispositivo de encaminamiento o la máquina de destino han encontrado en el datagrama.
- Se envían al origen de la transmisión

INFORMES DE ERROR:

- **Destino inalcanzable**
- **Frenar origen**: Surgen con los problemas de congestión, ocasionando que una máquina mande un mensaje ICMP de error a la máquina origen para que frene el tráfico de datos y así poder solucionar el problema.
- **Tiempo excedido**: Se produce cuando un paquete llega a una máquina y su TTL marca 1, con lo que ese paquete no puede salir de ella, o bien porque es la máquina destino o porque ese paquete ha sido descartado. Por ese motivo, manda a la máquina origen un mensaje de tiempo excedido.
- **Problemas con parámetros**
- **Redirección:** Ocurre cuando un paquete tira por un camino, pero se da cuenta que hay otro más corto, haciendo que alguna máquina que no se esperaba vea el contenido del paquete. Esta máquina manda un mensaje al origen para que se revise las tablas de encaminamiento.

No se generará un mensaje de error:

- En respuesta a un datagrama que lleve un mensaje de error ICMP.
- Para un datagrama fragmentado que no sea el primer fragmento.
- Para un datagrama que tenga una dirección multicast
- Para un datagrama que tenga una dirección especial (127.0.0.1)

MENSAJES DE MONITORIZACIÓN Y CONSULTA:

Sirven para diagnosticar problemas en la red y ayudan a obtener información específica acerca de un router u otra máquina. Además, se envían por pares debido a que un nodo envía un mensaje que es respondido por otro nodo destino.

Informes de consulta:

- **Petición de eco y respuesta**: Se utilizan para comprobar que una máquina está viva. Se manda un mensaje ICMP (de eco) y la máquina que lo recibe debe mandar otro con una copia del contenido del datagrama original.
- **Petición de marca de tiempo y respuesta**: Sirve como mensaje de diagnóstico. La máquina de origen manda un mensaje especial que incluye un código de 32 bits con la hora local de la máquina y la envía al destino. El destino lo recibe e incluye su propia hora y la vuelve a enviar a la de origen. De este modo, la máquina origen conoce el round-trip time, si los relojes están sincronizados y si las latencias son simétricas o no.
- **Petición de dirección de máscara y respuesta y Petición de router y anuncio**: Se encuentran obsoletas.

INTERCONEXIÓN DE REDES

Las redes de área local no se encuentran normalmente aisladas, sino que existen conexiones entre segmentos de una misma LAN, a otras LAN o a Internet.

Los dispositivos trabajan a distintos niveles y cuando hablamos de un nivel, nos referimos a que trabajan con la información a ese nivel, teniendo implementado los niveles inferiores y olvidándose de los superiores.

Existen cinco categorías dependiendo del nivel al que operen en la red:

NIVELES	**DISPOSITIVOS**
APLICACIÓN	PASARELA
TRANSPORTE	
RED	ENRUTADOR (ROUTER) O ENCAMINADOR DE TERCER NIVEL
ENLACE	PUENTE O ENCAMINADOR DE SEGUNDO NIVEL
FÍSICO	REPETIDOR O CONCENTRADOR

<u>INTERCONEXIÓN A NIVEL FÍSICO:</u>

- **Repetidores:**
  - Amplifican las señales eléctricas cuando se usan cables largos (no solo cables sino otros medios de transmisión física).
  - Solo copian los bits que recibe por su entrada en su salida.
  - Presentan algunas limitaciones:
    - Tienen límites de distancia
    - No interconectan redes de diferentes tipos
    - No realizan gestión de red
      - No es posible hacer una distribución del tráfico
      - No es posible introducir seguridad

- **Hubs (concentrador)**:
  - Es igual que el repetidor, pero presenta varias salidas. La señal que entra por una de sus entradas se copia y las envía por todas sus salidas.

INTERCONEXIÓN A NIVEL DE ENLACE:

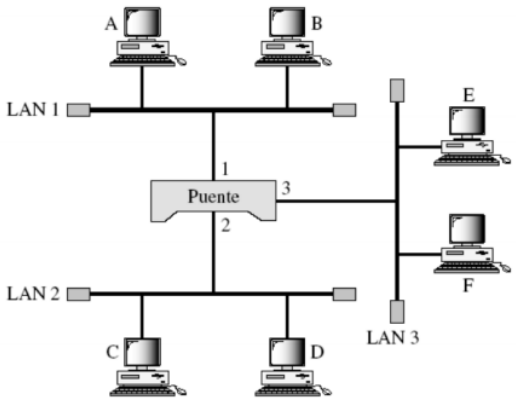
Si un dispositivo realiza una interconexión a **nivel de enlace**, **no presenta IP** porque no trabaja a nivel de red.

No realizan ningún tipo de modificación de la trama del nivel de enlace, solo la procesan para distribuir el tráfico.

- Conmutadores (switches):
  - Un conmutador interconecta máquinas.
- Puente (Bridge):
  - Un puente interconecta redes locales
  - Tienen implementado hasta el nivel de Enlace de Datos
  - Son dispositivos de almacén y envió
    - Aceptan una trama, verifican checksums, la analizan y se devuelve a la capa física para envío a la otra subred.
    - No permiten encaminar paquetes.
  - Las redes interconectadas se consideran una sola subred.
  - Tipo de puentes:
    - Trasparentes
      - Interconectan redes iguales
      - Dos tipos:
        - Básicos
        - De aprendizaje (Aísla tráfico)
    - De traducción
      - Conecta redes con protocolos diferentes a nivel de enlace (o MAC en el caso de las LAN).
      - Antes de reenviar las tramas realiza la conversión de protocolos que sea necesaria.

PUENTES TRANSPARENTES DE APRENDIZAJE:

- Tienen capacidad de filtrado (decide enviar o eliminar la trama)
- Decide por qué puerto realizar el envío
  - Mantiene tabla interna que relaciona direcciones y puertos



Dirección	Puerto

a. Original

Dirección	Puerto
A	1

b. Después de que A envié una trama a D

Dirección	Puerto
A	1
E	3

c. Después de que E envié una trama a A

Dirección	Puerto
A	1
E	3
B	1

d. Después de que B envié una trama a C