Unidad 1: Redes de Ordenadores e Internet

### Conceptos Generales

#### Tipos de redes

* **LAN:** Suelen ser redes privadas que ocupan un edificio.
* **MAN:** Red para una provincia o comunidad autónoma.
* **WAN:** Redes que abarcan un país o un continente. Internet se considera una WAN.

#### Componentes *Hardware* de una Red de Ordenadores

Elementos de comunicación:

* **HUB:** Recoge un paquete y lo envía a todos sus puertos.
* **Switch:** Analiza el paquete y solo lo envía a su/s destinatario/s. Analizan el tráfico a nivel de MAC.
* **Router:** Interconecta redes LAN, MAN y WAN. Analiza el paquete a nivel de IP y lo envía al destinatario correspondiente.

Elementos de transmisión:

* **Cable de cobre**
* **Cable de fibra óptica**
* **Aire**

#### Componentes *Software* de una Red de Ordenadores

Existen dos modelos de capas: OSI y TCP/IP.

### Arquitectura de Internet

#### Organismos que Dirigen Internet

IETF, IANA/ICANN, 3GPP.

### Modelo de Capas: OSI y TCP/IP

#### OSI

Modelo teórico de 7 capas: Aplicación, presentación, sesión, transporte, red, enlace, físico.

#### TCP/IP

* Capa **Aplicación**: Protocolos → HTTP (80), HTTPS (443), SSH (22), FTP (21 y 20), DNS (53), DHCP (67 y 68), SMTP…
* Capa **Transporte**: Protocolos → TCP y UDP.
* Capa **Red**: IP
* Capa **Enlace**: MAC
* Capa **Física**: Nivel de señal eléctrica, frecuencia, canal radio…

La comunicación es vertical, de la capa de aplicación (5) del ordenador uno va a la capa de transporte (4), así sucesivamente hasta la capa física (1) y de ahí a través de la red hasta la capa física (1) del ordenador 2, y de nuevo hasta la capa de aplicación (5) del ordenador 2.

### Preguntas de Test

##### Si hacemos PING al DNS de Google 8.8.8.8 ¿Qué paquetes veremos en Wireshark?

→ Paquetes de ping request a la IP destino 8.8.8.8 y paquetes de ping replay con IP origen 8.8.8.8

##### ¿Cuál es el protocolo más comúnmente utilizado para la transferencia de archivos en Internet?

→ FTP.

##### De las tres conectividades que dispone VirtualBox ¿Con cuál de ellas puede conectarse con Internet?

→ NAT y Adaptador Puente.

##### El IETF (Internet Engineering Task Force)

Publica los denominados RFC (Request for Comments).

Unidad 2: Nivel de Aplicación

### Funciones

Se encarga de unir al usuario con la red.

Contiene el software de aplicación que puede ser:

* Aplicaciones de Red: aquellas que utiliza la red para su propio funcionamiento como el servicio DNS o el DHCP.
* Servicios: Aplicaciones que utiliza el usuario. Firefox, servicio de correo, Teams, SSH…

### Aplicaciones sobre la Pila TCP/IP

Los protocolos como HTTP/S, SMTP/S, POP3/S, FTP, TELNET o SSH utilizan TCP para garantizar la entrega de los paquetes.

En cambio el DHCP y DNS usan UDP.

### Herramientas de Comprobación de la Disponibilidad de las Aplicaciones

En *Linux* podemos gestionar los servicios en ejecución en nuestra máquina con el comando **service**.

Con la herramienta **NMAP** podemos comprobar los servicios en ejecución de una máquina remota:

Ejemplo → nmap <servidor> -p<puerto> -s<protocolo de transporte T o U>

### Servicio de Navegación Web

Apache2 o Nginx ofrecen este servicio.

1. El cliente introduce una URL. Tras una resolución DNS se obtiene la IP del servidor WEB.
2. Se hace una conexión con el servidor (GET con HTTP o HTTPS). El servidor obtiene el contenido y se devuelve (200 OK HTTP o HTTPS).
3. La página web es presentada al cliente.

En Linux, la información de la web de nuestro servidor apache2 se encuentra en:

/var/www/html/index.html

### Servicio DNS

Su funcionamiento se basa en traducir los nombres de dominio tipo [www.u-tad.com](http://www.u-tad.com/) o [mail.telefonica.net](http://mail.telefonica.net/) en las IP de los servidores que ofrecen estos servicios.

#### Paquete BIND9 de Linux

Para crear un servidor DNS, podemos usar el paquete *bind9* de Linux. Una vez instalado, podemos configurar el servidor modificando los ficheros de configuración.

* **/etc/bind/named.conf.options:** fichero de configuración general.
* **/etc/bind/named.conf.local:** fichero de definición de la zona (dominio).
* **/etc/bind/db.<dominio>:** que se crea a partir de /etc/bind/db.local y que es el fichero de configuración de la zona (dominio).

Una vez configurados, con los siguientes comandos nos aseguramos de que tengan efecto estas configuraciones:

* **named-checkconf:** Comprueba que no hay errores de sintaxis en los ficheros de configuración del DNS.
* **named-checkzone:** Comprueba la sintaxis del fichero de zona, p.e. named-checkzone u-tad.uni /etc/bind/db.u-tad.uni.
* **rndc reload:** recargamos la base de datos.
* **service bind9 restart:** Reiniciamos el servidor de DNS.

### Otros Servicios

Para cada aplicación servidora se debe instalar su demonio correspondiente (apache2 o bind9) que permite dejar un servicio operativo, escuchando en el puerto correspondiente y esperando a un cliente (demonio Stand Alone).

#### INETD

INETD (super servidor de internet) es un demonio que se mantiene a la escucha de todas las peticiones que llegan al servidor y dependiendo del puerto que solicite, levanta el servicio correspondiente.

Permite optimizar recursos.

#### Servicios de Transferencia de Ficheros y Conexión Remota

* FTP: Permite transferir archivos entre sistemas. No encripta datos.
* Telnet: Permite la conexión remota. No encripta datos.
* **SSH:** Permite la conexión remota y la transferencia de archivos con cifrado.

### Preguntas de Test

##### La primitiva TTL=3600 segundos en un fichero de zona (DNS) ¿Qué significa?

→ Tras una consulta, el cliente lo guarda en caché y no vuelve a consultar por él hasta pasados 3600 segundos.

##### El servicio o demonio INETD lo utilizan los sistemas Linux para:

→ Hacer más óptima la ejecución de las aplicaciones servidoras, arrancando los servicios sólo cuando hay peticiones de los clientes.

##### Cuando instalamos un servidor WEB como puede ser Apache en una máquina que tiene la dirección IP (192.168.20.10) y además ese servidor sólo tienen activo ese servicio. ¿Qué presenta el comando: nmap 192.168.20.10 -p80 -sU?

→ Aparecerá la siguiente respuesta PORT STATE SERVICE : 80/udp closed http

→ Que el puerto 80 UDP está cerrado, ya que el servicio de páginas WEB sólo escucha en el puerto 80 TCP.

##### La siguiente entrada " u-tad.uni. IN NS ns.u-tad.uni." En el fichero de zona o fichero de registro de recursos indica que las URLs u-tad.uni y ns.u-tad.uni devuelven la misma IP cuando se consulta por ellas.

→ FALSO

Unidad 3: TCP-IP: Nivel de Transporte y Nivel de Red

### Funciones de la Capa de Transporte

#### Control de Errores

Los 3 aspectos básicos para asegurar una entrega fiable son:

* Detección de errores y retransmisión de los segmentos erróneos.
* Control de secuencia para detectar si se pierde información o si está dañada.
* Control de duplicados.

#### Direccionamiento de Aplicaciones – Puertos

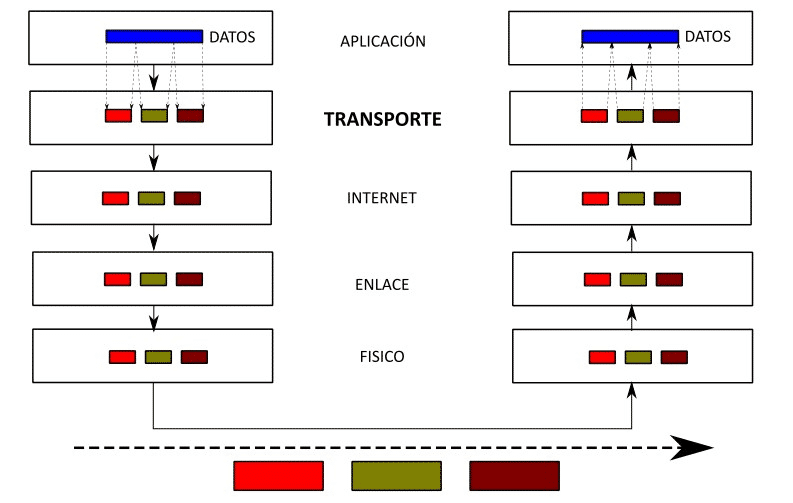
Los puertos se dividen en **tres rangos**:

* ***Well-Known Ports*** (0-1023): Son usados por aplicaciones específicas y deberían ser usados solo por estas (80, 443, etc.). Estos son asignados por la ***IANA*** (*Internet Assigned Numbers Authority*).
* *Registered Ports* (1024-49151): Se pueden asignar a una aplicación establecida por la *IANA* pero en la práctica cualquiera puede usarlos.
* *Ephimeral Ports* (49152-65535): Pueden usarse libremente como puerto origen. No están asignados a aplicaciones concretas.

#### Segmentación y Multiplexación

La segmentación o **paquetización** es el proceso donde (**remitente**) se **divide** el mensaje **en paquetes**, se agregan los puertos origen y destino en el encabezado de los mismos y se transfiere el mensaje a la capa de red.

En el lado del **receptor**, la capa de transporte recibe datos de la capa de red, vuelve a **ensamblar los paquetes**, lee su encabezado e identifica el número de puerto, conocido el puerto envía la información a la aplicación correspondiente.



La **multiplexación** optimiza el uso de los recursos de red al permitir la transmisión simultánea de múltiples flujos de datos sobre una (**ascendente**) o varias (**descendente**) conexiones, mejorando la eficiencia y la capacidad de comunicación.

#### Control de Flujo y de Congestión

El objetivo es evitar la pérdida de información por un emisor rápido y un receptor lento.

##### Control de Flujo

Normalmente se utiliza el **método de ventana deslizante** que significa que **el receptor informa al emisor de cuánta información es capaz de procesar** para que ajuste la cantidad de información que envía.

##### Control de Congestión

Se da cuando muchos equipos de una red envían datos y los routers comienzan a desbordarse perdiéndose paquetes.

* Control de Congestión de Bucle Abierto o soluciones pasivas: están para evitar la congestión.
* Control de Congestión de Bucle Cerrado o soluciones activas: actúan cuando se detectan problemas.

### Checksum

La forma que tienen los protocolos de detectar errores en los paquetes recibidos es a través del mecanismo de suma de verificación (*checksum*).

Se aplica en los protocolos UDP, TCP e IP.

##### En resumen:

Se hace la suma binaria de los bloques del paquete, se obtiene el complemento a uno (checksum) y se envían por la red tanto los bloques como el checksum.

Una vez en el receptor, se suman todos los bloques y el checksum y si:

* **El resultado son todo 1’s → Transmisión SIN errores.**
* **El resultado contiene algún 0 → Transmisión CON errores.**

### Protocolos de Transporte UDP/TCP

La conectividad en la capa de transporte se puede clasificar como orientada a la conexión *(Connection-Oriented)*, implementada en **TCP** o sin conexión *(Connectionless)*, implementada en **UDP**.

#### Protocolo UDP

Se utiliza para **transmitir datagramas de forma rápida** en redes IP y funciona como una alternativa sencilla y sin retardos del protocolo TCP. Se usa principalmente para consultas tipo **DNS** y para la **transmisión de audio y vídeo.**

* Ofrece la funcionalidad mínima requerida → Direccionamiento de aplicaciones.
* **Menos fiable** → No garantiza la entrega de los datagramas.
* **Sin estado** → Cada datagrama es independiente y no existe una conexión inicial.
* Es **rápido → No establece conexión inicial.**
* **Baja sobrecarga de red.**
* Usado en → **Comunicaciones de voz, DHCP, DNS, RIP…**

Los datagramas se intercambian mediante petición - respuesta. La cabecera incluye datos como el puerto origen y el destino, longitud del datagrama, checksum y los datos.

#### Protocolo TCP

* Con estado → La app que envía y la que recibe comparten contexto sobre la comunicación.
* Usa streams → conjunto de todos los paquetes.
* Más fiable.
* Usado en → Comunicaciones de texto (Whatsapp), transferencia de ficheros, navegación web, correo electrónico…

##### TRES FASES:

Al ser un protocolo orientado a la conexión, sigue estas tres fases:

1. **Conexión – Three Way Handshake:** Se sincronizan los números de secuencia para posteriormente usarlos para recuperar, ordenar y reenviar paquetes. Flags →SYN, SYN+ACK, ACK.
2. **Transmisión de la información:** Se envían los datos. TCP gestiona la pérdida de paquetes y el desorden de los mismos. Cada vez que se envía un paquete, el destinatario envía un ACK para confirmar que lo ha recibido.
3. **Desconexión – Teardown:** Flags → FIN, ACK y FIN, ACK.

### Funciones de la Capa de Red

Proporciona servicios para permitir que los dispositivos finales intercambien datos a través de redes. **El protocolo principal es el IP.**

##### FUNCIONES:

1. **Direccionamiento de Nodos:** Cada nodo tiene una IP única.
2. **Encapsulamiento:** Se agrega información de encabezado IP, como la dirección IP de los hosts de origen y destino.
3. **Routing / Enrutamiento:** Encamina los paquetes por la red de routers.
4. **Desencapsulamiento:** El nodo destino desencapsula la información.

**El protocolo IP utiliza UDP y existen dos versiones → IPv4 (32 bits) e IPv6 (128 bits).**

### Direccionamiento CIDR IPv4

#### Máscara de Red

La **máscara de red** es un componente esencial del direccionamiento IP que separa una dirección en dos partes: **red** y **host**. Su longitud es de **32 bits**, con los primeros bits en 1 para identificar la red y los restantes en 0 para los hosts. Se representa como */M*, donde M es el número de bits a 1. Por ejemplo, una máscara **/24** utiliza los primeros **24 bits** para la red.

#### CIDR en IPv4

El objetivo de CIDR es que a través de la **máscara variable** podamos crear tantas **subredes** como necesitamos asignando IPs de manera muy eficiente.

##### IPs Disponibles:

Se calcula como 2^BH siendo BH los bits de host. Ejemplo → para /24, tendríamos 2^8 ips (256) de las cuales 2 son reservadas para la red y para la broadcast (x.x.x.0 y x.x.x.255). Es habitual asignar la primera al router.

##### Dirección de Broadcast:

Se utiliza cuando queremos enviar información a todos los nodos de la red.

#### IPs Públicas e IPs Privadas

##### IPs ESTÁTICAS y DINÁMICAS:

* Estáticas: Se asignan de forma permanente. IPs para servidores.
* Dinámicas: Se asigna una diferente cada vez que un nodo se conecta a la red (portátil al conectarse a una WiFi).

##### IPs PÚBLICAS y PRIVADAS:

* Privadas: No pueden viajar por internet. Ejemplo → Todos los equipos de nuestra casa que están conectados a la WiFi.
* Públicas: IPs que tienen los nodos que se conectan a redes públicas como Internet.

### Otros Protocolos de la Capa de Red

#### Protocolo ICMP

Permite a los nodos enviar mensajes de información como errores o diagnósticos de red (**PING o** **traceroute**).

#### Protocolos de Routing (RIP, OSPF y BGP)

Los protocolos de routing **hacen posible que los routers se comuniquen**, intercambiando tablas de enrutamiento y haciendo que los paquetes vayan de un router a otro hasta el destino.

### Preguntas de Test

##### Si en una comunicación llegan los paquetes desordenados existen mecanismo en el software de las redes de ordenadores que pueden ordenarlos

→ Verdadero.

##### Si para codificar una dirección IPv4 se usan 32 bits cuantas IPs diferentes podemos tener

→ 2^32=4.294.967.296

##### En una comunicación si se pierde un paquete hay ciertos protocolos de transporte que pueden recuperarlos pero hay otros que no tienen esas capacidades.

→ Verdadero (TCP sí tiene pero UDP no).

##### Cuando se necesita una IP pública para un servidor tengo varias opciones

→ Usar un servicio como AWS donde previo pago tus servidores pueden tener IP públicas.

→ Solicitarla a un proveedor de Internet (ISP).

##### Si consideramos el modelo software TCP/IP creado por los padres de Internet, Robert Kahn y Vinton Cerf podemos decir que:

→ Fueron los cimientos y las primeras versiones del modelo TCP/IP actual que marca las comunicaciones en Internet.

##### Si al lanzar un ping a un equipo distante recibimos un mensaje ICMP con la descripción "TTL expired". ¿Qué puede estar pasando?.

→ Que ha expirado el TTL de los paquetes IP porque se han superado el número de saltos permitidos y el paquete de ida se ha descartado por algún router en Internet.

##### Al hacer un nslookup a la URL www.u-tad.com nos devuelve la IP 81.46.243.216. Dado que el servicio de página WEB de U-tad está visible en Internet, de la IP 81.46.243.216 que podemos decir que:

→ Se trata de una IP pública para que pueda usarse en Internet y los clientes desde cualquier parte del mundo puedan acceder a la WEB de la universidad.

→ Lo normal es que sea una IP estática para que no haya que estar continuamente actualizando los dominios en los DNS.

##### La cabecera UDP tiene cuatro campos principales: puerto origen, puerto destino, longitud y checksum cada uno de 16 bits. Si el campo longitud tiene el siguiente valor 0000.0000.0111.1111, ¿cuántos bytes tiene el Datagrama UDP incluyendo la cabecera y los datos?

→ 111.1111 en binario 127 bytes.

Unidad 4: Capa de Enlace y LAN Cableadas

### Funciones de la Capa de Enlace

Se encarga de ofrecer servicios a la capa de red y gestionar el envío y recepción de las tramas (*mensajes* encapsulados) con la capa física.

##### FUNCIONES:

1. **Construcción de las Tramas:** Encapsulación de los mensajes de la capa de red.
2. **Control de Enlace Lógico (LLC).**
3. **Control de Acceso al Medio (MAC).**
4. **Direccionamiento:** Cada nodo se identifica mediante la dirección MAC.
5. **Detección y corrección de errores.**

### Implementación de la Capa de Enlace

La capa de enlace y la capa física son los responsables de la velocidad y la latencia de la comunicación.

Algunos protocolos utilizados son:

* Redes LAN: Ethernet (IEEE 802.3), WiFi (IEEE 802.11)
* Redes WAN: PPP, HDLC, SDLC, ATM.

### Direcciones MAC

Es un número **hexadecimal** de **12 dígitos** (**48 bits**) integrado en la **tarjeta de red** (se graba durante la fabricación de la misma). Se llama también **dirección física**.

Ejemplo → 00:1A:2B:3C:4D:5E

#### Formato y Tipos de MAC:

Formato:

* Los primeros 6 dígitos identifican al fabricante (OUI).
* Los otros 6 dígitos representan el controlador de la interfaz de red (NIC).

Existen 3 tipos:

* **Unicast**: Si una trama tiene una dirección MAC destino unicast ésta sólo se envía al nodo que tiene esa MAC en su NIC.
* **Multicast**: La dirección de multicast permite al origen enviar una trama a un grupo de dispositivos.
* **Broadcast**: Las tramas direcciones destino **FF.FF.FF.FF.FF.FF** se denominan direcciones de broadcast, y llegarán a todos los equipos pertenecientes a ese segmento LAN.

### Protocolo ARP

El protocolo de resolución de direcciones ARPes un protocolo que **mapea una dirección IP a una dirección MAC** de una en una red **LAN**.

Sabemos la IP y MAC origen, la IP destino y necesitaremos este protocolo para conocer la MAC destino. El procedimiento es el siguiente:

1. El nodo emisor envía una **solicitud ARP** (que contiene la IP destino) a nivel de **broadcast**.
2. Todos los nodos de la LAN reciben la solicitud pero solo responde el dispositivo con esa IP devolviendo su MAC (**ARP replay**).
3. El nodo **emisor** **recibe** la **respuesta** y **guarda la MAC en caché**.

Ejemplo:

* A la ida la trama broadcast tienen MAC origen=49:BD:D2:C7:56:2A, MAC destino= FF:FF:FF:FF:FF:FF y mensaje *ARP Request* con IP=141.23.56.23
* A la vuelta la trama *unicast* tienen MAC origen=A4:6E:F4:59:83:AB, MAC destino=49:BD:D2:C7:56:2A y mensaje *ARP Replay* con MAC=A4:6E:F4:59:83:AB.

### Detección y Corrección de Errores

Para la detección de errores seguiremos utilizando **checksum** y además el algoritmo de **códigos de redundancia cíclica**.

Además, en la capa de enlace existen códigos de corrección de errores como:

* Códigos Hamming.
* Códigos Convolucionales Binarios.
* Códigos de Reed-Solomon.
* Códigos de Verificación de Paridad de Baja Densidad.

#### Código de Redundancia Cíclica (CRC)

Es un código mucho más complejo que el checksum ya que se realiza a nivel de hardware, lo que permite hacer operaciones más complejas.

Se basa en divisiones binarias XOR:

1. El emisor **divide** la trama por un valor especial llamado **polinomio generador**.
2. El **resto** de la división es el **CRC**. Se agrega a los datos y se envía.
3. El r**eceptor realiza la misma división**.

* Si el resto es **cero**, los datos llegaron **sin errores**.
* Si el resto es **distinto a cero**, los datos llegaron con **errores**.

### LAN Cableadas - Estándar Ethernet IEEE 802.3

Es una tecnología muy rápida que al principio proporcionaba 3MB, pero hoy en día llega a los 10GB.

Los principales **componentes** **hardware** de Ethernet son:

* Hub, Switch, Cables de Cobre, Cables de Fibra Óptica.

### Control de Acceso al Medio Ethernet CSMA/CD

En este algoritmo los dispositivos de red escuchan el medio antes de transmitir para determinar si los recursos están disponibles.

### Servicio DHCP

Este protocolo permite que un host obtenga una dirección **IP** de manera **automática** (la dirección **IP, la máscara, los DNS** y el **default gateway**).

El **puerto** que utiliza el **servidor** es el **67** y el **cliente** el **68** ambos **UDP**.

#### Proceso DORA

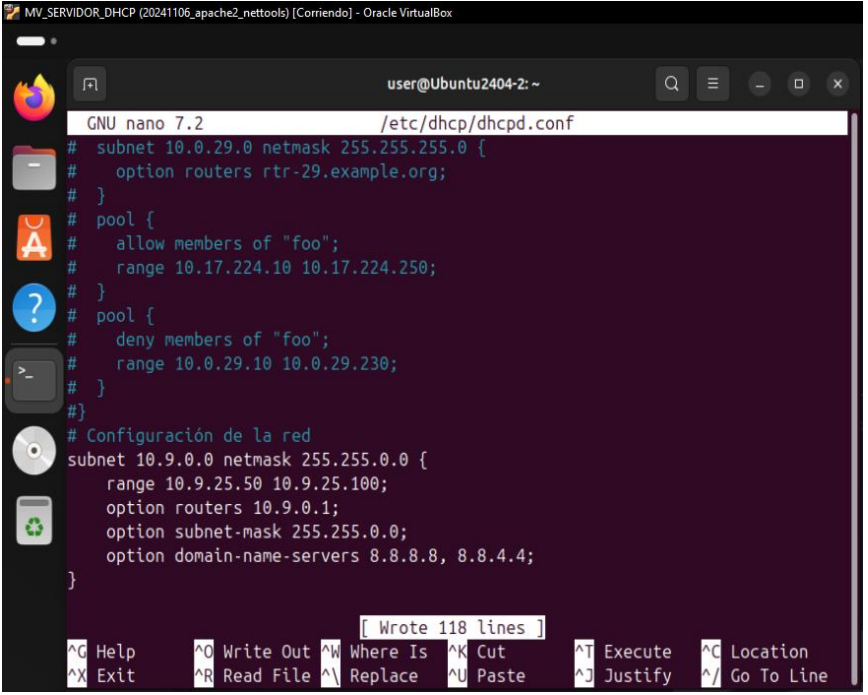
Es el proceso que se lleva a cabo entre cliente y servidor para usar DHCP:

1. **Discover:** Este primer mensaje lo genera el cliente para ver si hay un servidor DHCP en la red.
2. **Offer:** El servidor DHCP responde al cliente con un mensaje de oferta que contiene una IP a utilizar por el cliente.
3. **Request:** El cliente recibe la IP y envía un mensaje DHCP Request confirmando que acepta esa IP.
4. **Acknowledge:** El servidor envía un mensaje Acknowledge con la IP, máscara, puerta de enlace, DNS al cliente.

#### Paquete isc-dhcp-server de Linux

Para la configuración de un servidor DHCP se puede usar el paquete de linux ***isc-dhcp-server***.

Ejemplo de configuración en un servidor DHCP en ubuntu:



En wireshark, con el filtro dhcp podríamos ver los pasos del proceso DORA.

### Servicio NAT

El NAT es el mecanismo de Internet que traduce las direcciones IP privadas en públicas necesarias para acceder a internet.

El router que conecta la red local con Internet realiza esta traducción cambiando la **IP origen privada por su propia IP pública**. Cuando el paquete regresa, el router cambia la **IP destino pública por la IP privada del dispositivo original**, permitiendo la comunicación correcta.

NAT ayuda a ahorrar direcciones IP públicas y facilita la seguridad y la conectividad.

### Preguntas de Test

##### Cuando en una red Ethernet un nodo que tiene una MAC=00:0a:83:b1:c0:ff quiere enviar una mensaje de difusión a todos los nodos conectados a esa LAN construirá un mensaje con las siguientes características:

→ MAC origen=00:0a:83:b1:c0:ff – MAC destino=ff:ff:ff:ff:ff:ff (broadcast)

##### ¿Qué tipo de tecnología de red utiliza cables para la transmisión de datos?

→ Red de Área Local (LAN): Ethernet

→ Red WAN: Fibra óptica.

→ Red de Área Personal (PAN): Bluetooth

→ Red MAN: Token Ring

##### Si el fabricante de tarjetas Ethernet CISCO tiene asignado el OUI=cc:46:d6 y no tiene más OUIs, ¿cuántas tarjetas diferentes puede fabricar?

→ 2^24 (como cualquier fabricante que no tiene más OUIs)

##### Si un router que conecta una intranet privada (con IPs privadas) con Internet, cuyo interfaz con la intranet tiene IP=192.168.15.1 y MAC=00:1b:44:11:3a:b7 y el interfaz con Internet tiene IP=81.46.243.1 y MAC=00:fb:4a:48:3a:bb, además ese router hace las funciones de NAT. Si un equipo de la intranet con IP=192.168.15.20 con MAC=00:fa:5c:27:aa:b7 envía un ping al DNS de Google IP=8.8.8.8, ¿Cuál es la IP origen y la MAC origen de los paquetes que van hacia internet en el interfaz que conecta el router con Internet?

→ IP origen=81.46.243.1 – MAC origen=00:fb:4a:48:3a:bb (interfaz pública)

##### Si quiero que mi servidor de DHCP ofrezca a los clientes los DNS 80.58.61.250 y 80.58.61.254 y el rango de IPs a ofrecer sea 192.168.17.5 a 192.168.17.10, en el fichero de configuración o /etc/dhcp/dhcpd.conf debo escribir las siguientes primitivas

→ range 192.168.17.5 192.168.17.10; option domain-name-servers 80.58.61.250, 80.58.61.254;

##### El algoritmo CSMA/CD que permite el acceso al medio compartido (cable) de manera eficiente, cuando se produce una colisión

→ A los nodos que han colisionado se les hace esperar un tiempo aleatorio hasta que pueden volver a transmitir nuevamente, así se reduce estadísticamente la probabilidad de que vuelvan a colisionar.

Unidad 5: Redes inalámbricas: WiFi y Redes Móviles celulares (4G y 5G)

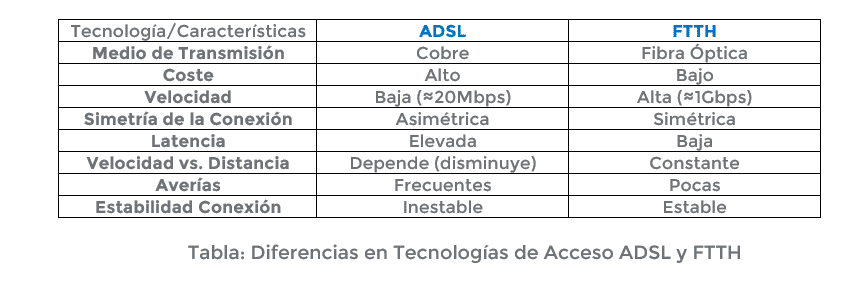
### Tecnologías de Redes de Acceso

Para poder navegar por Internet, es necesario que un proveedor de servicios (*ISP*) nos habilite el acceso. Este acceso puede ser tanto de acceso fijo como de acceso móvil.

* **Redes de Acceso Fijo**:

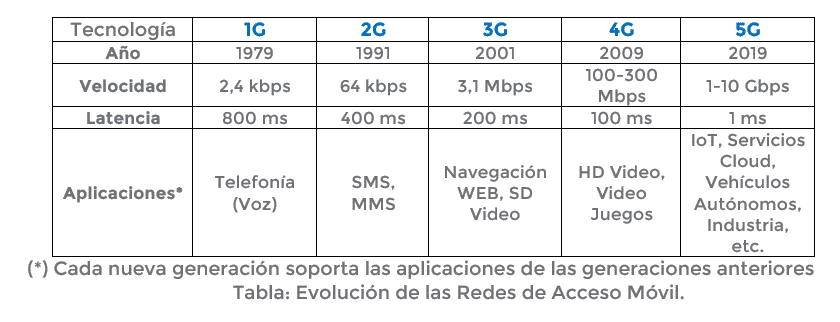
ADSL (**cobre**), FTTH (**Fibra Óptica**) o de Acceso Inalámbrico como el **Wi-Fi**.

El ISP conecta una línea de cobre o de fibra óptica hasta el sitio en el que se quiera conexión, y también instala un router donde a partir de él construimos nuestras LAN.



* **Redes de Acceso Móvil**:

1G, 2G, **3G, 4G o 5G**. No se necesita un router, solo una tarjeta **SIM**.



### Redes Inalámbricas

Se envían señales a través del aire.

#### Efectos No Deseados en los Canales Inalámbricos

* **Desvanecimiento**: La señal pierde fuerza cuando atraviesa materiales o se dispersa.
* **Ruido**: Dispositivos que usan frecuencias similares o fuentes de ruido ambiental (como microondas) generan interferencias que afectan la calidad de la señal.
* **Propagación Multitrayecto**: La señal rebota en objetos y llega al receptor por diferentes caminos, causando distorsión al recibir varias versiones de la misma señal en distintos momentos.

#### Soluciones a los Efectos No Deseados

Para las redes WiFi tenemos:

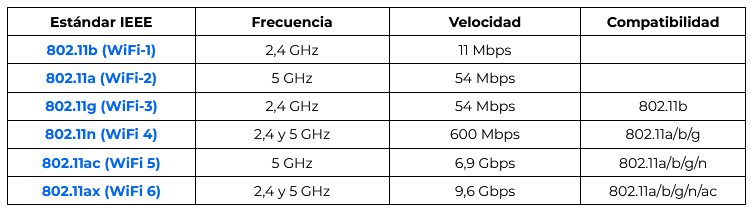
* DFS: Evita que se usen canales repetidos.
* Power Management: Ahorra energía y evita interferencias.
* Rate Adaptation: Mantiene una conexión estable adaptando la velocidad.

Para las redes móviles tenemos:

* **CSMA**: Es un sistema que permite a múltiples transmisores usar simultáneamente un mismo canal de comunicación y banda de frecuencias sin interferencias.
* MIMO: Se aprovecha de múltiples antenas de transmisión y recepción para sacar partido de la propagación multitrayecto

### Redes WiFi IEEE 802.11

Existen varios estándares 802.11 para WLAN.



Las dos bandas de frecuencias principales son la 2'4 GHz y la de 5 GHz. Ambas son de **uso libre y sin licencia**.

Además, todos estos estándares tienen varias características comunes:

* Todas son compatibles con sus versiones anteriores.
* Utilizan CSMA/CA.
* Misma estructura de tramas.
* Todos tienen la capacidad de reducir su velocidad de transmisión para abarcar más distancia.

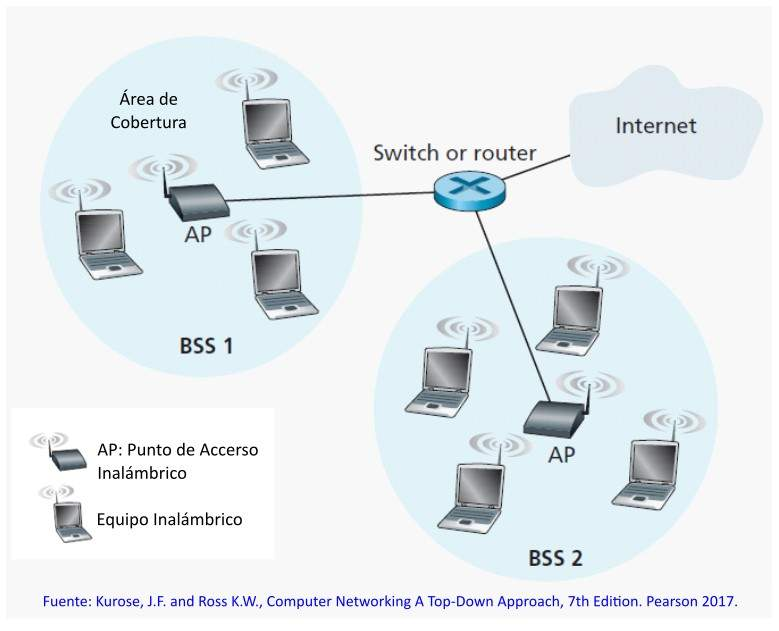
### Arquitectura de WLAN IEEE 802.11

**AP o Punto de Acceso Inalámbrico:**

Es el **dispositivo físico** que permite la comunicación inalámbrica entre los dispositivos inalámbricos y una red cableada.

**BSS o Basic Service Set:**

Es el área de cobertura de una WiFi. En él se encuentra el AP y varios dispositivos inalámbricos.

**BSSID o Basic Service Set Identifier:**

Es la MAC del AP (6 bytes).

**SSID o Service Set Identifier**

Es el nombre de la WiFi.

### Conexión a WLAN IEEE 820.11

El proceso para que un nodo inalámbrico pueda conectarse a una red WiFi es el siguiente:

1. **Escaneo:**

- Escaneo **Pasivo**: Los APs envían tramas *Beacon* para anunciarse y que los equipos inalámbricos las conozcan.

- Escaneo **Activo**: los equipos en lugar de escuchar pasivamente las señales de los AP, éstas envían una trama *Probe Request* para saber qué redes están disponibles. Las AP activas, responden afirmativamente con tramas *Probe Response*.

1. **Autenticación:** Se realiza Authentication Request y Authentication Response mediante los protocolos WPA o WPA2.
2. **Asociación:** Host se une al AP. Association Request Association Response.
3. **Transferencia de Datos.**

### Cabecera de la Trama IEEE 802.11

Destacar que a diferencia de la cabecera Ethernet que solo incluye 2 MAC esta incluye 4:

1. **Destination Address (DA):** dirección MAC del **nodo destino**.
2. **Source Address (SA):** dirección MAC del **nodo origen**.
3. **Receiver Address (RA):** dirección MAC del AP (**BSSID**).
4. **Transmitter Address (TA)**: dirección MAC del **nodo origen**.

### Control de Acceso al Medio

Estas redes usan un esquema de confirmación/retransmisión (ARQ) para garantizar la entrega de tramas sin errores.

#### Protocolo ARQ

1. Si el canal está libre, la estación transmite después de un breve retraso (DIFS).
2. Si el canal está ocupado, la estación elige un tiempo aleatorio y espera, pausando el conteo si el canal sigue ocupado.
3. Cuando el contador llega a cero y el canal está libre, la estación envía la trama y espera confirmación.
4. El receptor, tras un corto retraso (SIFS), envía la confirmación.
5. Si la estación recibe la confirmación, sabe que la trama fue recibida con éxito.

#### Protocolo CSMA/CA

Evita colisiones en una red inalámbrica.

Imaginemos que tenemos 3 nodos y un AP:

1. N1 quiere enviar datos, así que envía una trama **RTS (Request to Send)** para avisar a todas las estaciones, incluyendo el AP.
2. El AP responde con una trama **CTS (Clear to Send)** para autorizar la transmisión y notificar a las demás estaciones (como N2 y N3) que deben esperar para evitar colisiones.
3. N2 y N3 escuchan el CTS y se abstienen de transmitir durante el tiempo indicado.
4. N1 envía la trama de datos (**DATA**).
5. El AP confirma la recepción correcta enviando una trama de **ACK**.

### Redes Móviles Celulares: 4G y 5G

Cada vez van mejorando más en velocidad, latencia y fiabilidad.

La red **5G** nos abre puertas a nuevos servicios:

1. **Servicios de Banda Ancha Mejorada (eMBB).**
2. **Servicios de Comunicaciones Masivas (mMTC).**
3. **Comunicaciones Ultra Fiables y de Baja Latencia (URLLC).**

#### Espectro Radioeléctrico en Redes Celulares

**El espectro que utilizan las redes móviles es licenciado.**

### Preguntas de Test

##### El Multi-access Edge Computing consiste en…

→ …permite reducir la latencia poniendo los servidores a aplicaciones lo más cerca posible de los clientes.

##### Si un portatil 1 con MAC=c8:cb:9e:fd:a5:bb está enviando un paquete a otro portátil 2 con MAC=50:98:39:ee:f9:76 a través de un AP WiFi con BSSID=78:29:ed:9f:fb:7e. ¿Qué valores tienen los campos DA, SA, RA, y TA en la cabecera IEEE 802.11 en el tramo entre el portátil 1 y el AP?

→ DA (nodo destino)=50:98:39:ee:f9:76, SA (nodo origen)=c8:cb:9e:fd:a5:bb, RA(BSSID AP)=78:29:ed:9f:fb:7e y TA (nodo origen)=c8:cb:9e:fd:a5:bb

##### El despliegue de las redes 5G requieren mucha más inversiones que las redes WiFi principalmente por:

→ Coste de las licencias de espectro y despliegue de un volumen importante de antenas para tener cobertura nacional.

##### El proceso para que un nodo inalámbrico pueda conectarse a una red WiFi es el siguiente:

→ 1) Escaneo, 2) Autentificación, 3) Asociación y 4) Transferencia de datos.

##### ¿Qué característica principal diferencia a la tecnología 5G de las generaciones anteriores?

→ Mayor ancho de banda

UNIDAD 6: Seguridad en Redes de Ordenadores

##### 