UD5 – SISTEMES INFORMÀTICS EN XARXA-II

1º DAW - CFGS

Prof. Manuel Enguidanos
menguidanos@fpmislata.com

5.1.3. MAPES FÍSICS I LÒGICS DE XARXES

5.1. Redes informáticas

5.1.3. Mapas físicos y lógicos de una red

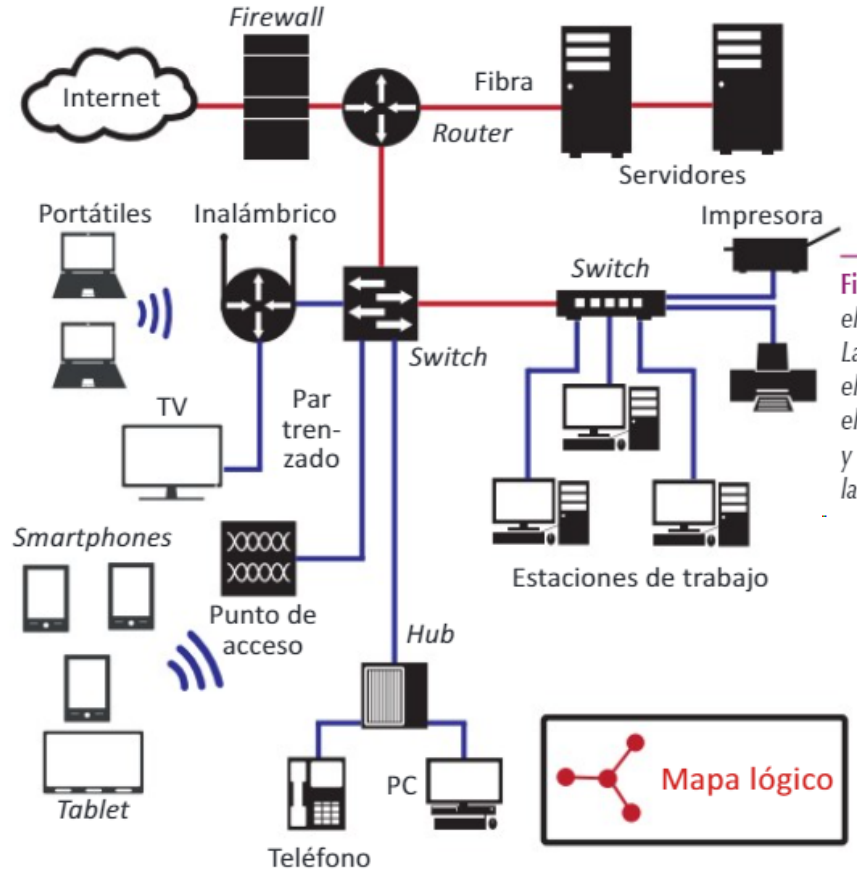
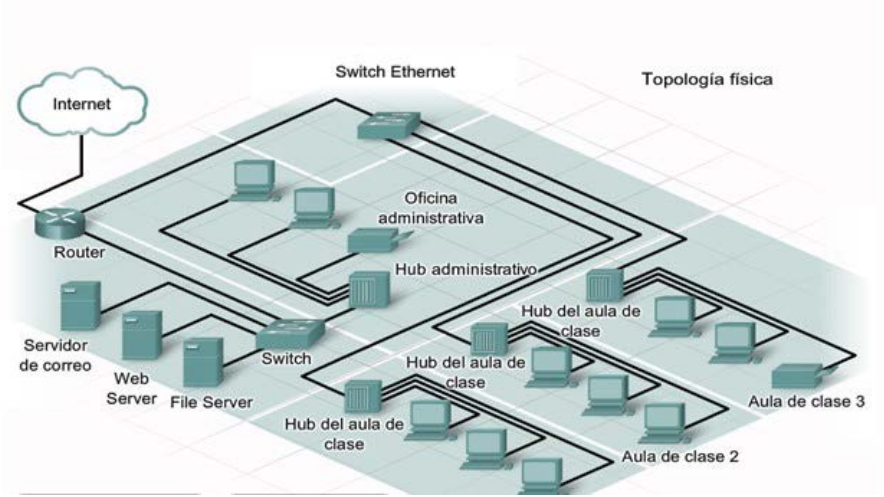
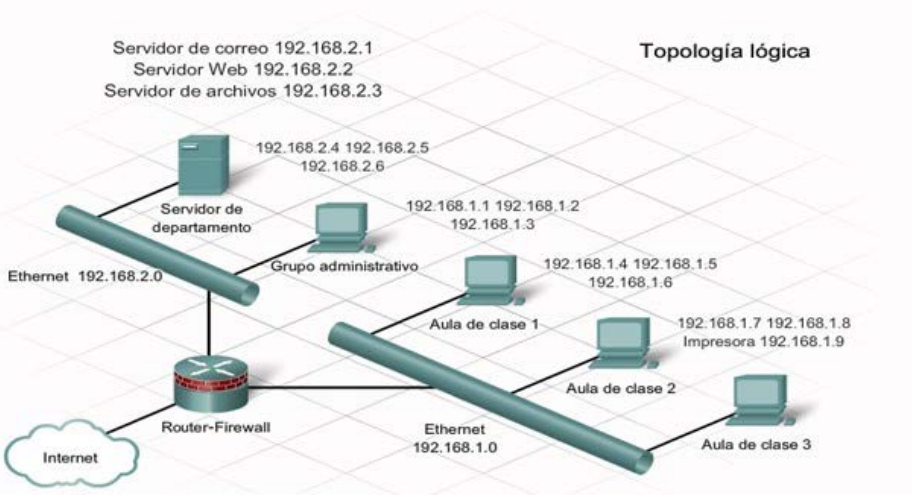


Figura 5.20. *Esquema básico con los elementos dentro de una red local. Se puede observar el cableado en color rojo como fibra óptica y el cableado en color azul como par trenzado. Las señales inalámbricas permiten la conexión de los portátiles,* smartphones *y* tablets *hacia el* router *inalámbrico y el punto de acceso inalámbrico. El* router *conecta la red local hacia el exterior (internet) a través del* firewall *y separa la red mediante fibra en la zona de los servidores y el* switch *troncal, que se conecta mediante fibra óptica a la zona de las impresoras y las estaciones de trabajo y mediante par trenzado o wifi con el resto de los equipos de la red.*

5.1. Redes informáticas

5.1.3. Mapas físicos y lógicos de una red





5.2. MODELOS DE REFERENCIA

5.2. Modelos de referencia

5.2.1. Modelo OSI

El modelo **OSI** (***O**pen **S**ystems **I**nterconnection,* interconexión de sistemas abiertos) es un modelo teórico de referencia utilizado para la interconexión de diferentes tipos de sistemas. Está formado por una serie de siete niveles, donde cada uno tiene una función bien definida que lo diferencia de los demás. Cada nivel se comunica con los adyacentes añadiendo una serie de cabeceras o información a los paquetes que se trasladen verticalmente a través de los niveles.

Capa o nivel	Función
Aplicación	Permite a las aplicaciones acceder a las demás capas.
Presentación	Cifra y comprime los datos.
Sesión	Permite a los usuarios establecer más de una sesión.
Transporte	Se asegura y confirma que los datos han llegado a su destino.
Red	Encamina de la manera más adecuada (óptima) los datos por la red.
Enlace	Agrupa los datos y se encarga de que no haya errores en la transmisión.
Física	Se encarga de todo lo relativo a la parte física de la transmisión.

5.2. Modelos de referencia

5.2.2. TCP/IP

El modelo TCP/IP está compuesto por cuatro capas o niveles que realizan una función similar a las capas del modelo OSI. Cada capa realiza una función para preparar el envío y la recepción de los datos a través de una red. Es el utilizado en las redes LAN.

El nombre del modelo TCP/IP hace referencia a los dos protocolos más importantes del modelo: el protocolo **TCP** (***T**ransmission **C**ontrol **P**rotocol*, protocolo de control de la transmisión) y el protocolo **IP** (***I**nternet **P**rotocol*, protocolo de internet).

Capa o nivel	Función
Aplicación	Se encarga de lo relacionado con los datos del usuario, del envío y recepción.
Transporte	Se dividen los datos y se crean paquetes.
Internet	Envía los paquetes por la red y establece la mejor ruta.
Acceso a la red	Se encarga de lo relacionado con el envío físico de los paquetes.

5.2. Modelos de referencia

5.2.3. Comparación entre los modelos OSI y TCP/IP

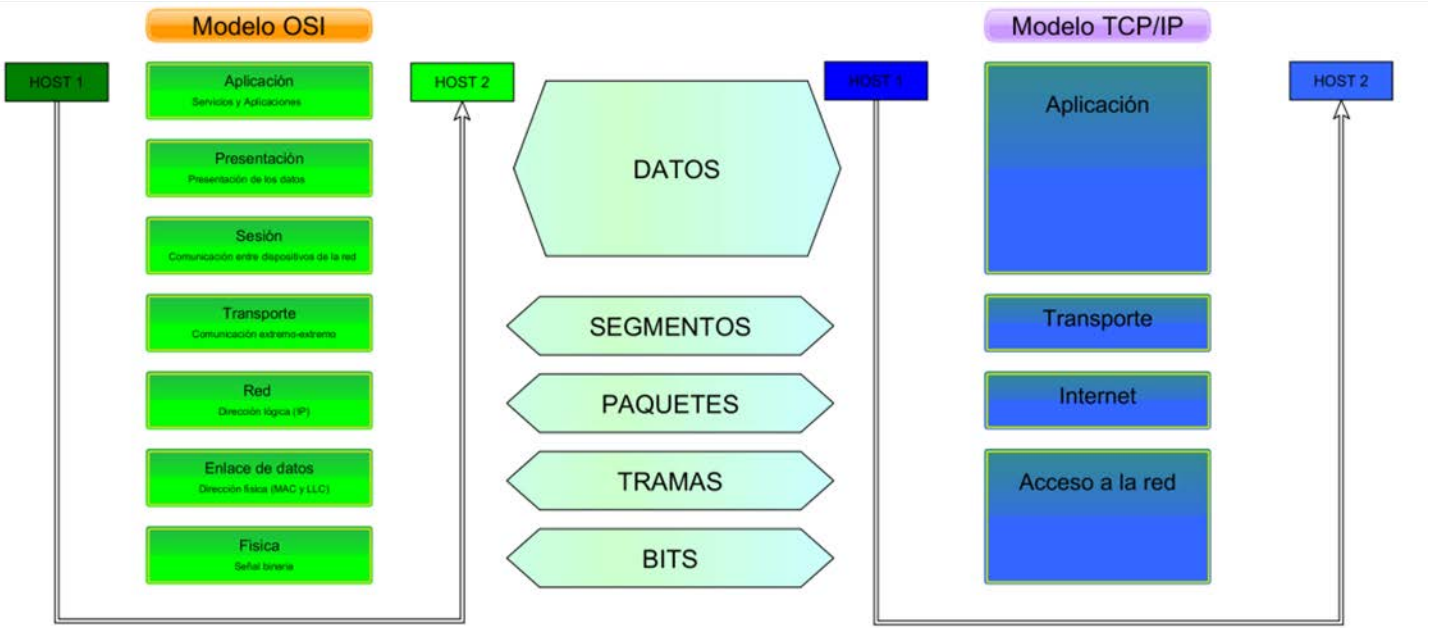
En ambos modelos la información del usuario viaja desde la capa superior a la inferior en el envío de los datos, viajan por la red, y en el destino la información va desde la capa inferior a la superior.

El usuario envía los **datos** desde la capa de aplicación a la capa de transporte, donde se dividen en **segmentos** (TCP) o **datagramas** (UDP) y se les añade una cabecera; posteriormente se les añade otra cabecera IP para indicar dónde enviar esos **paquetes,** que finalmente viajan en **tramas** por el medio físico.

TCP/IP	OSI
Aplicación	Aplicación
	Presentación
	Sesión
Transporte	Transporte
Internet	Red
Acceso a la red	Enlace
	Físico

5.2. Modelos de referencia

5.2.3. Comparación entre los modelos OSI y TCP/IP



5.2. Modelos de referencia

5.2.4. Protocolos utilizados en las redes

- **Aplicación.** En esta capa o nivel se pueden destacar los protocolos mencionados en la Tabla 5.5.

Tabla 5.5. Diferentes protocolos de la capa de Aplicación con la función que realizan

Nombre	Función
DNS	Protocolo del sistema de nombres de dominio.
DHCP	Protocolo de configuración dinámica de la red.
HTTP, HTTPS	Protocolos web.
FTP, TFTP	Protocolos de transferencia de ficheros.
SMTP, POP, IMAP	Protocolos de correo electrónico.
LDAP, LDAPS	Protocolos de los servicios de directorios.
Telnet, SSH	Acceso remoto y acceso remoto con seguridad.
SMB/CIFS	Protocolo para compartir archivos e imprimir.
NFS	Protocolo para acceder remotamente a archivos y directorios.
SNMP	Protocolo usado para la gestión de la red.

5.2. Modelos de referencia

5.2.4. Protocolos utilizados en las redes

- **Transporte.** Este nivel tiene los protocolos siguientes:
  - **TCP** (***T**ransmisión **C**ontrol **P**rotocol,* protocolo de control de la transmisión) se encarga de crear conexiones y garantiza la entrega de los datos.
  - **UDP** (***U**ser **D**atagram **P**rotocol,* protocolo de datagramas de usuario) es un protocolo que no requiere conexión y envía la información a través de mensajes o datagramas.
  - **SCTP** (***S**tream **C**ontrol **T**ransmission **P**rotocol,* protocolo de transmisión de control de flujo) reúne características de los dos anteriores. Está orientado a la conexión y la transferencia la realiza transmitiendo mensajes.
  - **TLS** (***T**ransport **L**ayer **S**ecurity,* seguridad de la capa de transporte) se utiliza para la transferencia de la información entre sitios web de forma segura y cifrada, para que la información que viaja por la red no pueda ser interceptada ni modificada. Es una subcapa que se encuentra entre los niveles de aplicación y transporte, ya que trabaja con muchos protocolos de la capa de aplicación añadiendo seguridad a los mismos. Su antecesor es **SSL** (***S**ecure **S**ocket **L**ayer,* capa de conexión segura).

5.2. Modelos de referencia

5.2.4. Protocolos utilizados en las redes

- **Internet.** En el caso de esta capa, los protocolos existentes son estos otros:
  - **IPv6** y **IPv4** (***I**nternet **P**rotocol,* protocolo de internet) son los protocolos encargados de encaminar los datos a través de su dirección IP. No están orientados a la conexión y trabajan con datagramas.
  - **IPSec** incorpora seguridad a los protocolos IP. Es un conjunto de protocolos que se encarga de asegurar el cifrado y la autenticidad de los paquetes.
  - **ARP** (***A**ddredd **R**esolution **P**rotocol,* protocolo de resolución de direcciones) y **RARP** (*Reverse ARP*, ARP inverso) se utilizan para conocer la dirección IP de un *host* a través de la MAC o al revés.
  - **ICMP** (***I**nternet **C**ontrol **M**essage **P**rotocol,* protocolo de mensajes de control de internet) se utiliza para enviar mensajes de control entre redes. Se utiliza para ver si hay conexión entre dos nodos y para comprobar la latencia.
  - **IGMP** (***I**nternet **G**roup **M**anagement **P**rotocol,* protocolo de gestión de grupos de internet) se utiliza para gestionar la multidifusión en las redes.

5.2. Modelos de referencia

5.2.4. Protocolos utilizados en las redes

- **Acceso a la red.** Sus protocolos son los siguientes:
  - **Ethernet** es el protocolo para acceder al medio. Todos los nodos comparten el mismo canal, es de difusión y un mensaje puede llegar a todos los nodos.
  - **Wifi** es un protocolo para acceder al medio en las redes inalámbricas.
  - **PPP** (***P****oint to* ***P****oint* ***P****rotocol,* protocolo punto a punto), **PPPoE** (***PPP o****ver* ***E****thernet,* PPP sobre Ethernet) y **PPPoA** (***PPP o****ver* ***A****TM,* PPP sobre ATM) son protocolos para las conexiones punto a punto.

5.2. Modelos de referencia

5.2.4. Protocolos utilizados en las redes

Modelo TCP/IP				Modelo OSI		
4	Datos	APLICACIÓN	HTTP, FTP, SMTP, POP3, IMAP (Protocolos)	APLICACIÓN	Datos	7
				PRESENTACIÓN		6
				SESIÓN		5
3	Segmentos	TRANSPORTE	TCP, UDP **SSL, TLS, WTLS** (Puertos)	TRANSPORTE	Mensajes	4
2	Datagramas IP	INTERNET	IP, IPX, APPLETALK , ARP, RARP, ICMP, IGMP, X.25, MPLS **IPSec**	RED	Paquetes	3
1	Tramas	ACCESO A LA RED	Direccionamiento físico y control. LLC: HDLC, LAPB, LAPF, PPP MAC: Ethernet, WiFi, ATM, Token Ring, Frame Relay, MPLS	ENLACE DE DATOS	Tramas	2
	bits		Transmisión binaria Cable coaxial, par trenzado, fibra óptica, conectores.	FÍSICA	bits	1

5.2. Modelos de referencia

5.2.4. Protocolos utilizados en las redes

Número de puerto

Cada protocolo suele trabajar en un número de puerto por defecto. Los puertos son un número entero que utiliza TCP/IP para identificar la aplicación a la que debe enviar y de la que debe recibir los paquetes y los datos que se envían por la red.

En general, no puede haber dos aplicaciones escuchando un mismo puerto. Por ejemplo, para tener dos servidores web en funcionamiento, se puede hacer que cada uno escuche en un número de puerto diferente. Cuando se accede a ese servidor se indican la dirección IP (que identifica al equipo dentro de la red) y el número de puerto (que identifica a la aplicación dentro del servidor). El conjunto de dirección IP y número de puerto se denomina ***socket.***

5.2. Modelos de referencia

5.2.4. Protocolos utilizados en las redes

Número de puerto

Puertos bien conocidos de TCP/UDP

Puerto preasignado	Protocolo	Aplicación
80	TCP	HTTP
21	TCP/UDP	FTP
23	TCP/UDP	Telnet
25	TCP/UDP	SMTP
110	TCP/UDP	POP3
119	TCP/UDP	NNTP
137	TCP/UDP	serv. de nombres NetBIOS
161	TCP/UDP	SNMP
194	TCP/UDP	IRC
389	TCP/UDP	LDAP
396	TCP/UDP	NetWare sobre IP
458	TCP/UDP	Apple QuickTime
500	TCP/UDP	ISAKMP

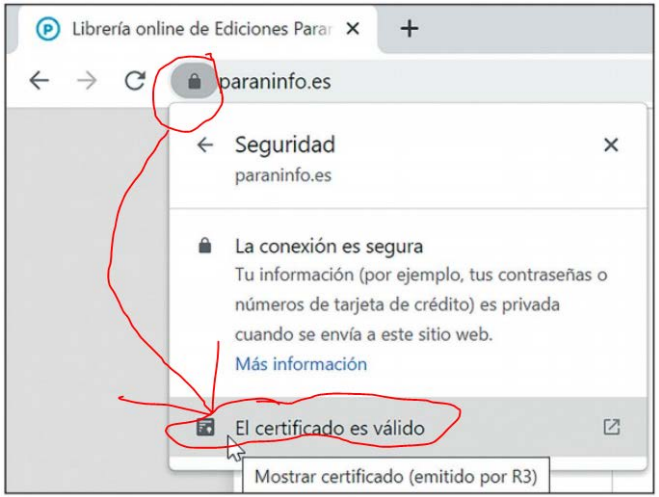
5.2. Modelos de referencia

5.2.4. Protocolos utilizados en las redes

Protocolo de transferencia de hipertexto (transferencia de información)

HTTP (***H**yper**t**ext **T**ransfer **P**rotocol,* protocolo de transferencia de hipertexto) y **HTTPS** (HTTP sobre SSL/TLS) permiten la transferencia de información desde un servidor con archivos de tipo HTML. El cliente usa un navegador web para ver la información. HTTP utiliza por defecto el puerto 80, mientras que HTTPS utiliza el 443.

HTTPS (***H**yper**t**ext **T**ransfer **P**rotocol **S**ecure,* protocolo seguro de transferencia de hipertexto) es la versión segura de HTTP. Utiliza un certificado SSL, la transferencia es cifrada a través de la red y solamente el navegador y el servidor web pueden descifrarla (Figura 5.22). El certificado debe estar instalado en el servidor.



5.2. Modelos de referencia

5.2.4. Protocolos utilizados en las redes

Transferencia de ficheros

El protocolo **FTP** (***F**ile **T**ransfer **P**rotocol,* protocolo de transferencia de archivos) se utiliza para transferir archivos entre equipos. En la capa de transporte utiliza el protocolo TCP. Utiliza por defecto el puerto 21.

TFTP *(**T**rivial **FTP**)* es un protocolo FTP que funciona bajo el protocolo UDP, con lo cual es simple, rápido, pero tiene algunas restricciones y es menos seguro, no asegura la descarga o subida libre de errores y se suele utilizar en archivos pequeños y cuando no se requiera mucha seguridad. Por defecto utiliza el puerto 69.

5.2. Modelos de referencia

5.2.4. Protocolos utilizados en las redes

Conexión remota (acceso a equipos remotos)

- **Telnet** es un protocolo no seguro que escucha por defecto el puerto 23. Al ser tan poco seguro casi no se usa en la actualidad, siendo sustituido por el siguiente.
- **SSH** (***S****ecure* ***Sh****ell,* protocolo de intérprete de órdenes seguro) es un protocolo seguro, que ha venido a sustituir al anterior. Trabaja por defecto en el puerto 22. Se utiliza para acceder a equipos de forma remota mediante un intérprete de órdenes o comandos. Además del acceso remoto tiene otras funciones, como la de transferir ficheros de forma segura utilizando el protocolo **SFTP,** o crear un canal seguro para intercambiar información entre equipos. SSH genera una clave pública y otra privada. La clave pública se envía al destino y allí se asocia a la cuenta de origen.

5.2. Modelos de referencia

5.2.4. Protocolos utilizados en las redes

Protocolos de escritorio remoto

- **VNC (*V**irtual **N**etwork **C**omputing*, computación virtual en red). Protocolo de escritorio remoto de *software* libre. Se puede utilizar con diversas aplicaciones en sistemas operativos Linux, Windows y macOS. Utiliza por defecto el puerto 5900.
- **RDP** (***R**emote **D**esktop **P**rotocol*, protocolo de escritorio remoto). Protocolo desarrollado por Microsoft. Utiliza por defecto el puerto 3389. Se puede utilizar en Linux con XRDP, que es una implementación de *software* libre de este protocolo.

5.2. Modelos de referencia

5.2.4. Protocolos utilizados en las redes

Protocolos de correo electrónico

- **SMTP** y **SMTP seguro (SMTP sobre TLS/SSL)** se utilizan para enviar correos electrónicos desde una aplicación cliente de correo. Utiliza por defecto el puerto 464 (o 25), y el 587 en su forma segura.
- **POP3** y **POP3 seguro (POP3 sobre TLS/SSL)** se utilizan para recibir correos electrónicos desde una aplicación cliente de correo. Utiliza por defecto el puerto 110, y el 995 en su forma segura.
- **IMAP** e **IMAP seguro (IMAP sobre TLS/SSL)** se utilizan en lugar de POP3 para no descargar los correos desde el servidor en el equipo propio, sino trabajando con ellos en el servidor. Utiliza por defecto el puerto 143, y el 993 en su forma segura.

5.2. Modelos de referencia

5.2.4. Protocolos utilizados en las redes

Protocolo para compartir recursos

- **RCP** (***R**emote **C**op**y***) se utiliza en los sistemas Linux. No es seguro, por lo que se recomienda alguno de los siguientes.
- **SCP** (***S**ecure **C**opy **P**rotocol*) es la versión segura del protocolo anterior; utiliza RCP sobre SSH.
- **RSYNC** permite copiar y sincronizar carpetas remotas.

5.2. Modelos de referencia

5.2.4. Protocolos utilizados en las redes

Protocolos de directorio activo

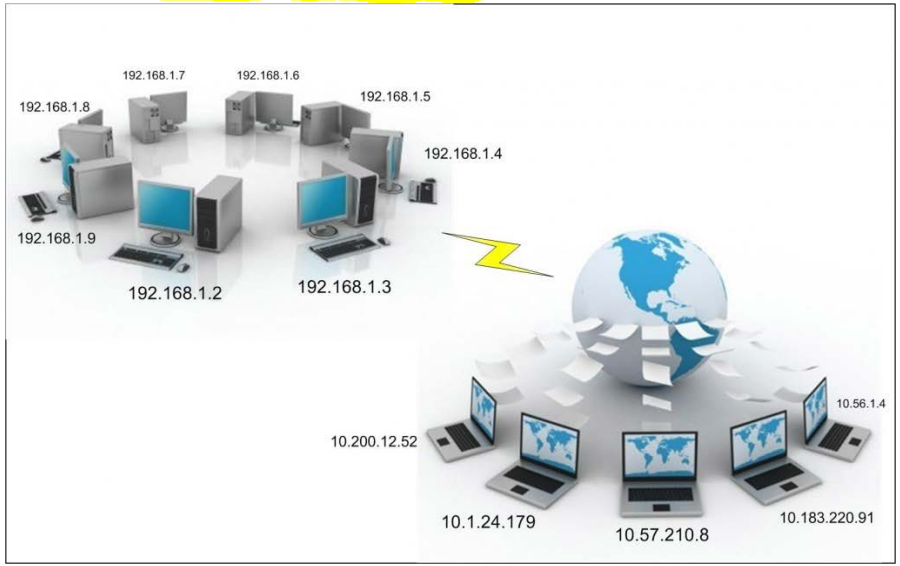
Se utilizan para iniciar sesión en los ordenadores a través de la red. Sirven para controlar quién se puede conectar y quién tiene acceso a determinados recursos. El protocolo de servicio de directorio activo y su variante con seguridad son **LDAP** (***L****ightweight* ***D****irectory* ***A****ccess* ***P****rotocol,* protocolo ligero de acceso a directorios) y **LDAPS.** En Windows este protocolo lo usa Active Directory y en Linux se instala a través de OpenLDAP. Utiliza los puertos predeterminados 389 y 636 para la versión segura.

5.3. DIRECCIONAMENT

5.3. Direccionamiento

Para el correcto funcionamiento de una red, esta debe estar correctamente direccionada de manera que se identifique de forma única cada nodo de la red. Para un correcto direccionamiento en una red es preciso configurar la dirección IP y la máscara de subred.

Otros elementos que son necesarios a la hora de mejorar el direccionamiento, para conectar diferentes redes entre sí o para acceder a otros equipos, serían la puerta de enlace o *gateway* y los servidores DNS y DHCP.



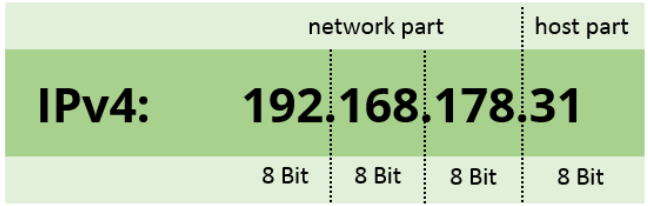
5.3. Direccionamiento

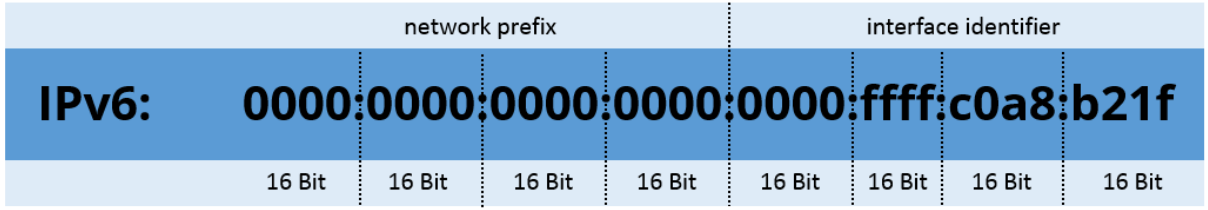
5.3.1. Direcciones IP

IPv4	IPv6
Implementado en 1981	Implementado en 1998
Dirección IP de 32 bits	Dirección IP de 128 bits
4300 millones de direcciones Las direcciones se deben reutilizar y enmascarar	$7{,}9 \times 10^{28}$ direcciones Todos los dispositivos pueden tener una dirección exclusiva
Notación numérica con punto decimal 192.168.5.18	Notación hexadecimal alfanumérica 50b2:6400:0000:0000:6c3a:b17d:0000:10a9 (Simplificada - 50b2:6400::6c3a:b17d:0:10a9)
Configuración DHCP o manual	Permite la configuración automática

5.3. Direccionamiento

5.3.1. Direcciones IP





5.3. Direccionamiento

5.3.1. Direcciones IP

Dirección IPv6 (en hexadecimal)

2a00:de40:0010:0313:0000:0000:0000:0105

ó

2a00:de40:0010:0313::0105

- Los dos puntos duplicados «::» representan los ceros omitidos

0010101000000000:1101111001000000:0000000000010000:0000001100010011:
0000000000000000:0000000000000000:0000000000000000:0000000100000101

5.3. Direccionamiento

5.3.1. Direcciones IP

Dirección de *loopback* o de bucle local

La dirección de *loopback* o de bucle local se utiliza para hacer referencia a la interfaz de red propia. Sirve para conectarse al equipo propio a través de aplicaciones y servicios que utilizan TCP/IP.

En IPv4 se suele utilizar la dirección `127.0.0.1`, aunque se puede utilizar cualquier dirección de la red 127.0.0.0 con máscara de subred 255.0.0.0. Para IPv6 se utiliza `::1`.

Para referirse a la dirección de *loopback* por el nombre, en los sistemas se utiliza la palabra `localhost`, que viene a significar *host* o equipo local.

Esta dirección se utiliza mucho para desarrollar y probar el *software* antes de alojarlo en un sitio web o para probar servidores locales.

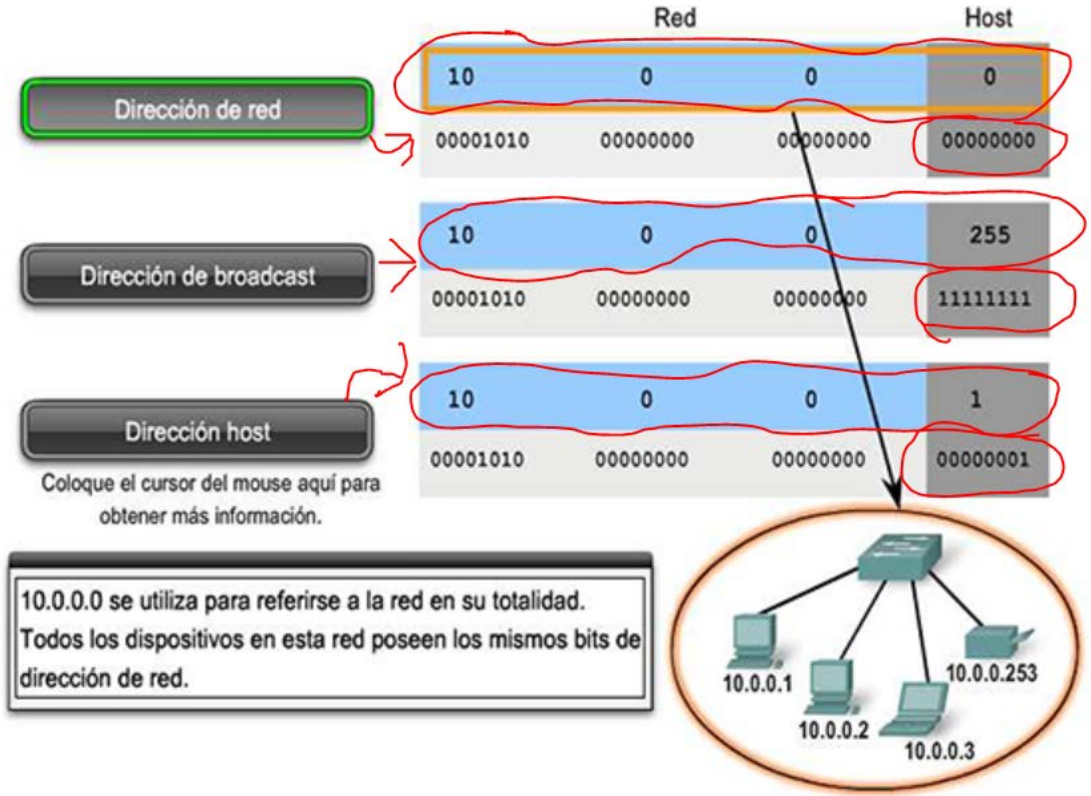
5.3. Direccionamiento

5.3.1. Direcciones IP

- **Dirección de red**: la dirección en la que se hace referencia a la red.
- **Dirección de broadcast**: una dirección especial utilizada para enviar datos a todos los hosts de la red.
- **Direcciones host:** las direcciones asignadas a los dispositivos finales de la red.

5.3. Direccionamiento

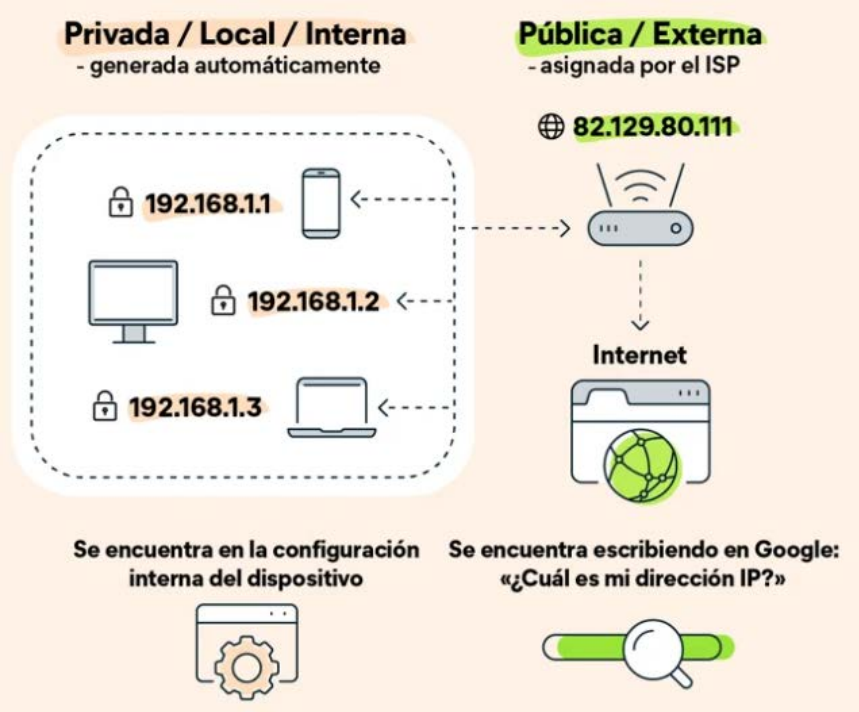
5.3.1. Direcciones IP



5.3. Direccionamiento

5.3.1. Direcciones IP

Direcciones IP públicas y privadas



5.3. Direccionamiento

5.3.2. Máscara de subred

Se utiliza en una dirección IP para diferenciar entre la parte de la dirección que identifica a la red y la parte que identifica a cada *host* de la red. También se puede utilizar para dividir una red en subredes. En IPv4 la máscara de subred tiene 32 bits, al igual que las direcciones IPv4.

La máscara de subred se puede expresar en forma de dirección IPv4 (decimal con puntos) o bien con la notación **CIDR** (***C**lassless **I**nter-**D**omain **R**outing*, enrutamiento entre dominios sin clases). Dependiendo del valor de la máscara de subred, se tendrán los bits destinados a la red y los bits destinados a equipos o *hosts* que se indican en la Tabla 5.6.

Máscara de subred	CIDR	Bits de red	Bits de *hosts*
255.255.255.0	/24	24	8
255.255.0.0	/16	16	16
255.0.0.0	/8	8	24

Se puede obtener la dirección de la red realizando una operación AND entre la dirección IP y la máscara de subred. Si la dirección IP del equipo es 192.168.0.32 y la máscara de subred es 255.255.255.0, para saber la dirección de la red se realiza la operación AND entre ambas direcciones:

```
        192.168.  0.32        11000000.10101000.0000000.00100000
AND     255.255.255. 0        11111111.11111111.1111111.00000000
        192.168.  0. 0        11000000.10101000.0000000.00000000
```

5.3. Direccionamiento

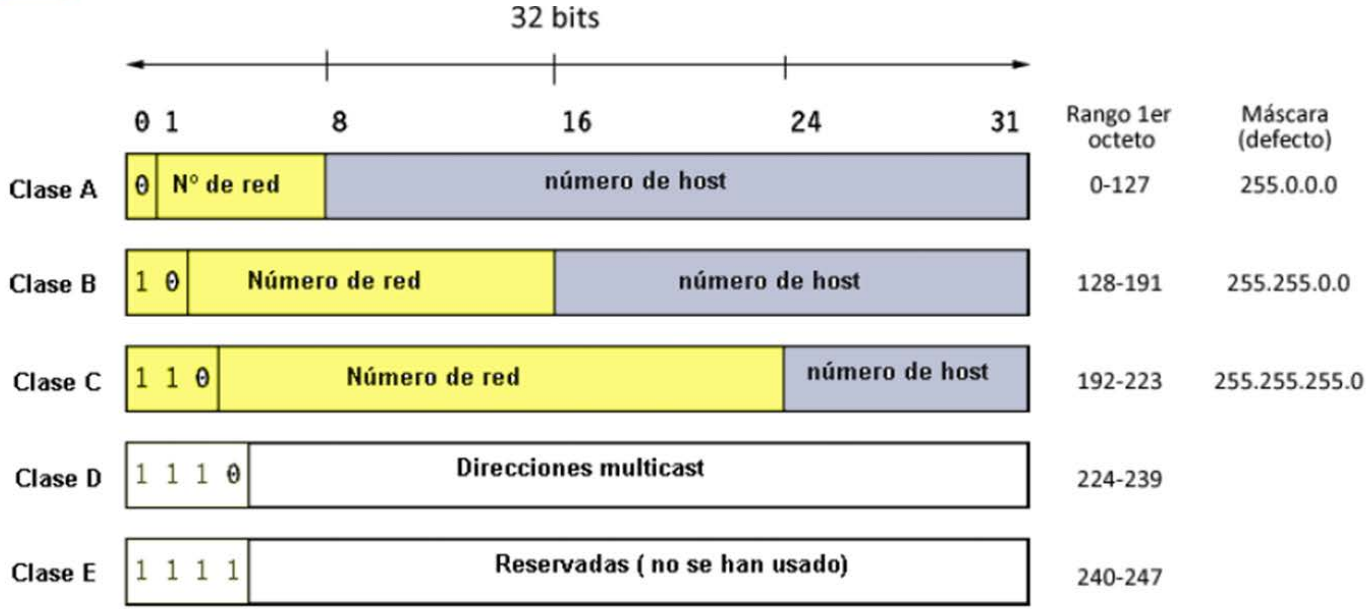
5.3.3. Clases de redes IPv4

Según el rango de direcciones se puede establecer la clasificación de las redes IPv4 que se muestra en la Tabla 5.7.

Clase	Intervalo	Bits de red	Bits de *hosts*	Máscara de subred	Dirección de *broadcast*
A	0.0.0.0 127.255.255.255	8	24	255.0.0.0 /8	x.255.255.255
B	128.0.0.0 191.255.255.255	16	16	255.255.0.0 /16	x.x.255.255
C	192.0.0.0 223.255.255.255	24	8	255.255.255.0 /24	x.x.x.255
D	224.0.0.0 239.255.255.255	Utilizada para multicast			
E	240.0.0.0 255.255.255.255	Redes experimentales y para investigación			

5.3. Direccionamiento

5.3.3. Clases de redes IPv4

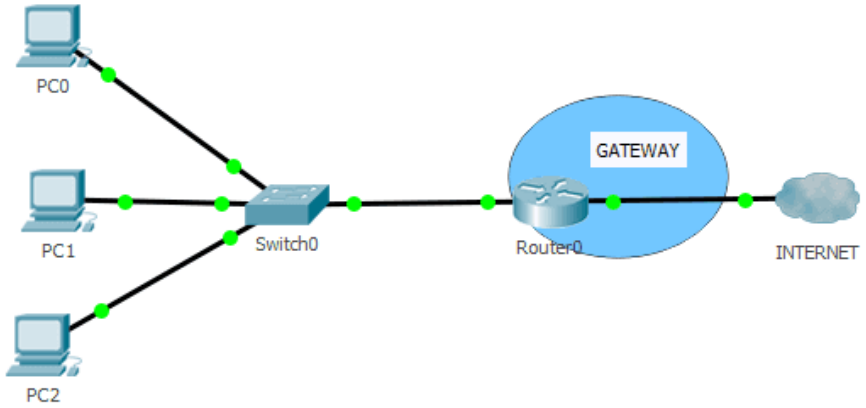


5.3. Direccionamiento

5.3.4. Puerta de enlace

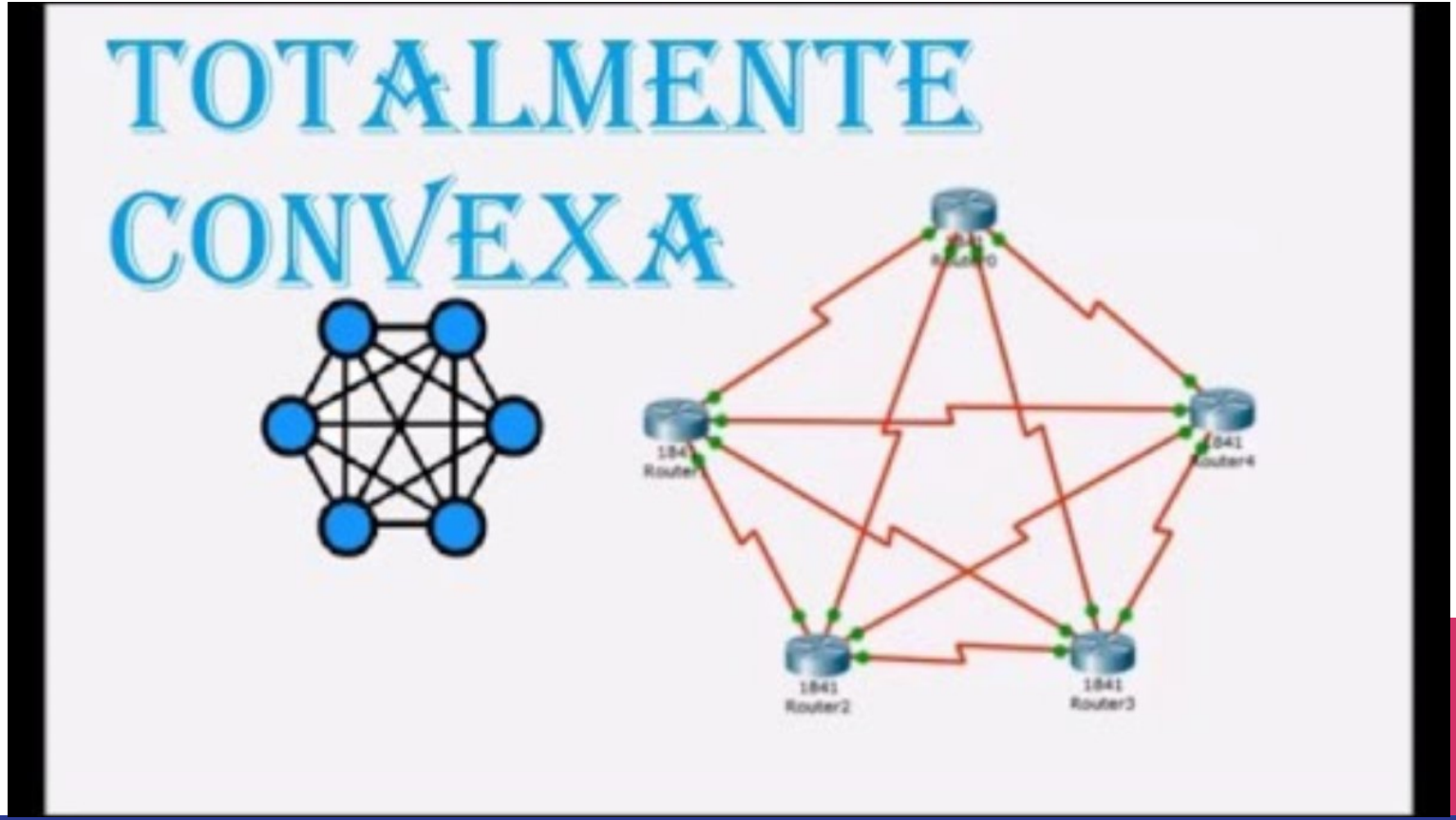
La puerta de enlace o *gateway* es la dirección IP del dispositivo que permite conectar dispositivos con protocolos diferentes. En una red local indicará la dirección del dispositivo que proporciona salida a internet; en una red pequeña, como las redes domésticas o de una pequeña empresa, suele ser un *router* con un módem incorporado.

Para acceder al *router* hay que conocer su dirección IP que, por defecto, suele ser 192.168.0.1 o 192.168.1.1. Se necesitará además un nombre de usuario y una contraseña.



Realitzar Pràctica 2

Realitzar Pràctica 2



https://www.youtube.com/watch?v=92OsBDfStvA

Realitzar Pràctica 2

https://www.youtube.com/watch?v=W30UwD2c6UM

UD5 – SISTEMES INFORMÀTICS EN XARXA-II

1º DAW - CFGS

Prof. Manuel Enguidanos
menguidanos@fpmislata.com