

COMPUTER SYSTEMS
UNIT8: COMPUTERIZED NETWORK SYSTEMS

CFGS DAM
DPT INF

UD8 SISTEMAS INFORMÁTICOS EN RED. CONFIGURACIÓN Y EXPLOTACIÓN

1. Protocolos principales de red.....	3
1.1. Protocolo Ethernet (capa OSI física).....	6
1.2. Protocolo Wi-Fi (capa OSI física).....	7
1.3. Protocolo IPv4 e IPv6 (capa OSI red).....	8
A) Protocolo IPv4.....	8
B) Protocolo IPv6.....	11
1.4. Protocolo TCP y UDP (capa OSI transporte).....	12
2. Configuración del protocolo TCP/IP.....	13
2.1. Estática.....	13
2.2. Dinámica.....	14
3. Interconexión de redes. Componentes.....	15
3.1. Switch (capa OSI enlace de datos).....	16
3.2. Router. Tablas de enrutamiento (capa OSI red).....	16
3.3. Topología física y lógica. Mapas.....	18
A) Topología física.....	18
B) Topología lógica.....	19
3.4. Dominios de colisión y difusión.....	20
4. Tipos de redes.....	21

COMPUTER SYSTEMS
UNIT8: COMPUTERIZED NETWORK SYSTEMS

CFGS DAM
DPT INF

5.	Acceso a redes WAN. Tecnologías	22
5.1.	Conexiones WAN privadas	22
5.2.	Conexiones WAN públicas.....	23
6.	Redes cableadas.....	24
6.1.	Tipos y características	24
A)	Cable de cobre par trenzado	25
B)	Cable de fibra óptica.....	27
6.2.	Dispositivos de interconexión	28
6.3.	Adaptadores.....	29
7.	Redes inalámbricas	30
7.1.	Tipos y características	30
A)	Wi-Fi	30
B)	WiMAX.....	31
C)	Sistemas de comunicación móvil 4G y 5G.....	31
D)	Otras redes WPAN.....	31
7.2.	Dispositivos de interconexión	32
7.3.	Adaptadores.....	33
8.	Ficheros de configuración de red	34
9.	Monitorización y verificación de una red mediante comandos.....	37
9.1.	Gestión de puertos	40
10.	Resolución de problemas.....	42
11.	Seguridad en las comunicaciones.....	44
11.1.	Políticas de seguridad.....	45
11.2.	Tipos de ataques.....	46
11.3.	Mecanismos de seguridad en las comunicaciones	46

COMPUTER SYSTEMS
UNIT8: COMPUTERIZED NETWORK SYSTEMS

CFGS DAM
DPT INF

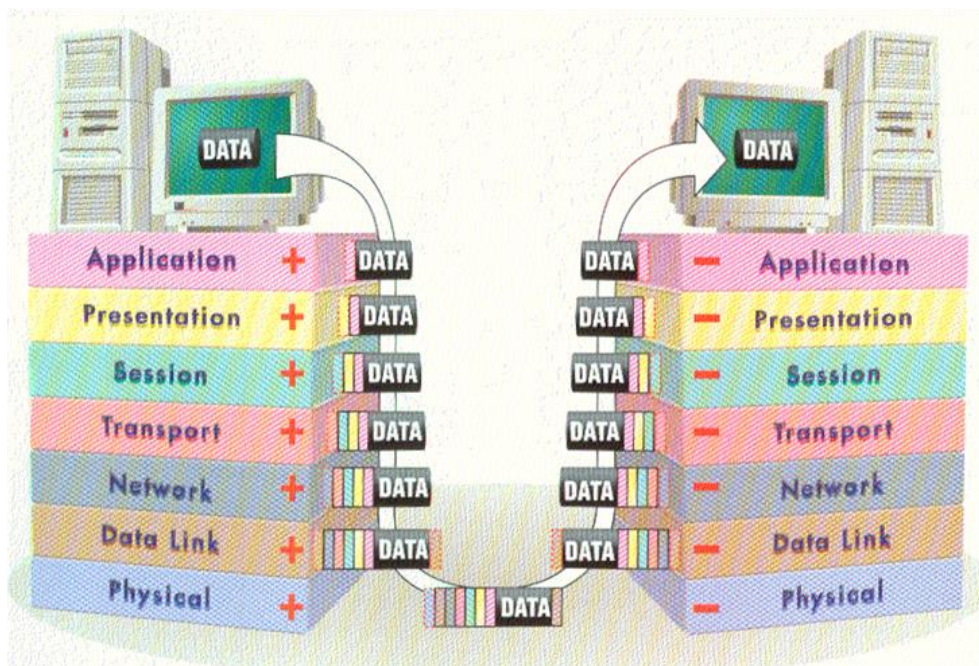
1. Protocolos principales de red

Los sistemas informáticos actuales se pueden considerar sistemas en red. Prácticamente no existe distinción hoy en día, ya que cualquier sistema informático con un sistema operativo que trabaje con un hardware específico de red y conectado con otros elementos de red con objeto de compartir información, forma parte de una red de comunicaciones.

Los sistemas informáticos en red se basan en **modelos de referencia**, que establecen las características y especificaciones necesarias para poder comunicarse entre diferentes entidades e intercambiar información. Estos modelos de referencia utilizan **arquitecturas de red** diferentes que descomponen sus funciones en varios niveles para definir protocolos y estándares, reducir la complejidad, controlar los flujos de comunicación y facilitar su evolución.

Los modelos de referencia más utilizados son el **modelo de referencia OSI** y el **modelo de referencia TCP/IP**.

El modelo de referencia OSI determina las funciones de comunicación de manera clara, dividiéndose en siete niveles. Cada nivel se corresponde con una capa que se comunica con su inmediata superior e inferior, de tal manera que el proceso de comunicación entre un emisor y un receptor sigue el recorrido que se muestra en la siguiente imagen.



COMPUTER SYSTEMS
UNIT8: COMPUTERIZED NETWORK SYSTEMS

CFGS DAM
DPT INF

Cada capa aporta una traza con metainformación necesaria para su interpretación en el receptor. A este proceso se le denomina encapsulamiento, en el que cada capa añade a los datos de la capa superior información asociada al protocolo que representa, constituyendo unidades de paquetes de datos (**PDU**). Así, cuando el flujo de bits llega al receptor, deberá liberarse del encapsulamiento en la capa correspondiente hasta llegar a la más alta.

Las capas y su función son las siguientes:

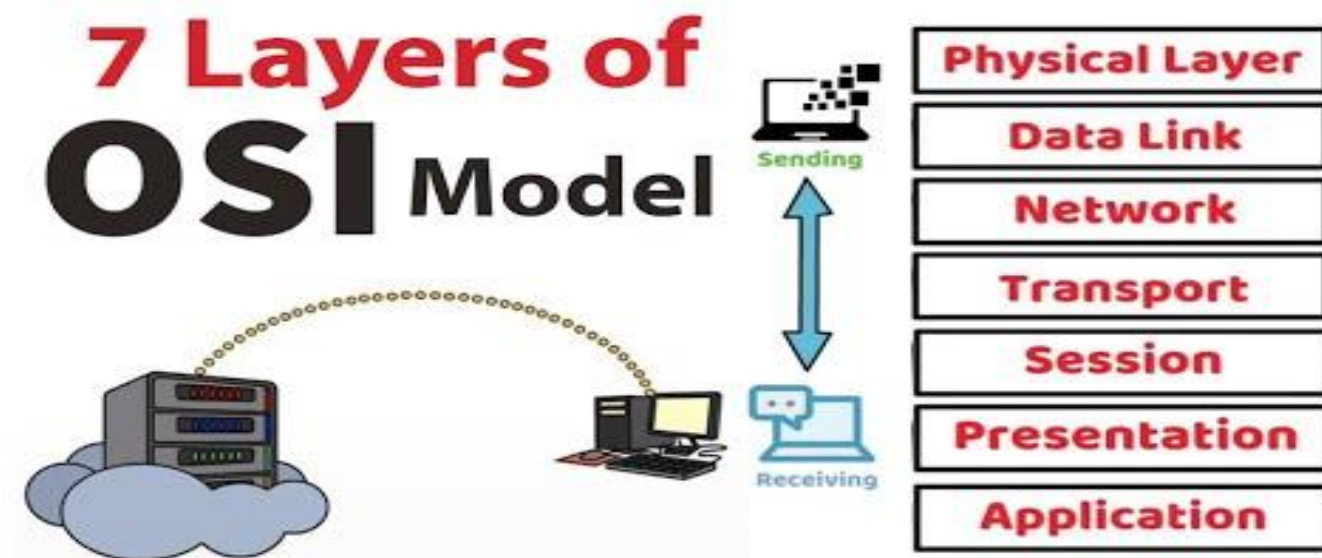
- **Aplicación.** Actúa de interfaz entre el usuario y las propias aplicaciones: navegadores web, aplicaciones de transferencia de ficheros, correo electrónico, terminales de red, exploradores de archivos, etc.
- **Presentación.** Determina el formato de la información para transferir entre las aplicaciones emisora y receptora. Codifica los datos, pudiendo comprimirlos o cifrarlos.
- **Sesión.** Define los mecanismos para establecer, mantener y controlar el diálogo entre las aplicaciones emisora y receptora. Las tres capas más altas no tienen un nombre concreto para sus PDU, por lo que se llaman datos en las tres.
- **Transporte.** Prepara y controla el flujo de datos entre emisor y receptor. Encapsula los segmentos de los datos de la capa de sesión.
- **Red.** Encargada de seleccionar la ruta entre el emisor y receptor. Encapsula los segmentos de datos en paquetes.
- **Enlace de datos.** Establece mecanismos de detección y corrección de errores en la transmisión de datos. Encapsula los paquetes en tramas.
- **Física.** Determina las especificaciones mecánicas, eléctricas y funcionales que establece y mantiene el enlace físico de transmisión. La trama, constituida por bits, se traduce en señales eléctricas, electromagnéticas o pulsos de luz, hasta que llegan al receptor, donde se vuelven a convertir en ceros y unos.

Las 4 capas inferiores se encargan del transporte y el control del flujo de datos, mientras que las 3 superiores están relacionadas con las aplicaciones (el host).

[OSI Model animated, What is osi model in networking? 7 OSI layers explained](#)

COMPUTER SYSTEMS
UNIT8: COMPUTERIZED NETWORK SYSTEMS

CFGS DAM
DPT INF



A diferencia del modelo OSI, el modelo TCP/IP no es solo un modelo conceptual y genérico, sino que constituye el estándar abierto de Internet. El modelo TCP/IP se adapta al modelo OSI, o viceversa, de tal manera que existe una correspondencia entre las capas de ambos como se muestra en la imagen.

Correspondencia entre los modelos OSI y TCP/IP

Modelo OSI	Modelo TCP/IP
7. Aplicación	a) Aplicación
6. Presentación	
5. Sesión	
4. Transporte	b) Transporte
3. Red	c) Internet
2. Enlace de datos	d) Acceso a red
1. Física	

COMPUTER SYSTEMS UNIT8: COMPUTERIZED NETWORK SYSTEMS

CFGS DAM
DPT INF

El nombre del modelo TCP/IP hace referencia a los protocolos más importantes empleados en el modelo: TCP e IP. Cada capa del modelo tiene asociados multitud de protocolos. Muchos de ellos los conocemos por sus siglas y otros son más desconocidos. En el cuadro siguiente se muestran algunos de ellos.

Protocolos destacados del modelo TCP/IP

Protocolo	Utilidad	Capa
<u>HTTP (Hypertext Transfer Protocol)</u>	Web	APLICACIÓN
<u>HTTPS (Hypertext Transfer Protocol Secure)</u>		
SMTP (Simple Mail Transfer Protocol)	Correo electrónico	
POP3 (Post Office Protocol 3)		DESCARGA
IMAP (Internet Message Access Protocol)		
DHCP (Dynamic Host Configuration Protocol)	Obtención de direcciones IP	
<u>DNS (Domain Name System)</u>	Traducción de nombres de dominio a direcciones IP	TRANSPORTE
FTP (File Transfer Protocol)	Transferencia de archivos	
FTPS (File Transfer Protocol Secure)		
TLS (Transport Layer Security)	Encriptación	INTERNET
SSL (Secure Sockets Layer)		
<u>UDP (User Datagram Protocol)</u>	Conexión y envío de información entre hosts	
<u>TCP (Transmission Control Protocol)</u>		ACCESO A LA RED
IP (Internet Protocol)	Enrutamiento de paquetes	
<u>NAT (Network Address Translation)</u>	Traducción de direcciones IP privadas a públicas	
<u>ARP (Address Resolution Protocol)</u>	Correspondencia entre direcciones MAC e IP	TRANSMISIÓN
<u>RARP (Reverse Address Resolution Protocol)</u>		
ETHERNET	Transmisión por cableado	
WLAN (Wireless Local Area Network)	Transmisión por Wi-Fi	
FDDI (Fiber Distributed Data Interface)	Transmisión por fibra óptica	

1.1. Protocolo Ethernet (capa OSI física)

Establece una forma de conexión y transmisión de datos por cable donde se especifican las características del cableado y su señalización, así como el formato de las tramas de datos. Está asociado a la capa física del modelo OSI.

Esta tecnología emplea un mecanismo llamado **CSMA/CD** (acceso múltiple por detección de portadora y detección de colisiones) en un medio compartido por varios hosts. El host que desee transmitir ha de

COMPUTER SYSTEMS
UNIT8: COMPUTERIZED NETWORK SYSTEMS

CFGS DAM
DPT INF

escuchar el medio previamente. Si está ocupado el canal, espera un tiempo antes de volver a intentarlo. Si 2 hosts transmiten a la vez, se producirá una colisión y ambos detendrán la transmisión.

La principal ventaja de Ethernet es su bajo coste, flexibilidad y facilidad en su implementación y seguridad ante accesos no permitidos. Por ello, es la más empleada en redes de área local (LAN).

Ethernet se corresponde con el estándar **IEEE 802.3**, el cual se divide en multitud de versiones con diferente ancho de banda para cable coaxial, cable de par trenzado y cable de fibra óptica.

1.2. Protocolo Wi-Fi (capa OSI física)

La tecnología Wi-Fi define un conjunto de especificaciones para redes de área local inalámbricas, asociándose a la capa física del modelo OSI. La familia **IEEE 802.11** establece multitud de estándares de transmisión de datos por radiofrecuencia en las bandas ISM¹ con fines no comerciales.

La familia de protocolos Wi-Fi emplean el mecanismo **CSMA/CA** (acceso múltiple por detección de portadora y prevención de colisiones) que, **a diferencia de CSMA/CD**, antes de transmitir, envía una notificación sobre su intención de hacerlo y, si recibe autorización, lo hace. Por tanto, se reduce considerablemente la probabilidad de colisiones en el medio.

Su principal ventaja es la facilidad en su instalación y la movilidad. Sin embargo, sus principales inconvenientes son la inseguridad al ser el medio de transmisión abierto y la saturación de los canales, donde se sitúan las bandas de 2,4 GHz y 5GHz, creando interferencias y, por lo tanto, aumentando la latencia en las comunicaciones.

Los estándares Wi-Fi mejoran con el paso del tiempo a sus antecesores, siendo los más utilizados los siguientes.

¹ El uso del espectro radioeléctrico para comunicaciones a distancia está regulado por los gobiernos nacionales. De este modo, los operadores de telefonía móvil, por ejemplo, deben pagar grandes cantidades de dinero para la explotación comercial de determinadas bandas de frecuencia.

Sin embargo, existen unas bandas de frecuencia, reservadas internacionalmente, que están libres de licencia. Estas bandas se pueden usar para objetivos no comerciales y, aunque no hay que pagar por usarlas, sí fijan unas condiciones de buen uso para garantizar la posible coexistencia de distintos sistemas.

Estas son las bandas ISM, siglas del inglés: industrial, scientific and medical. Se pueden utilizar para usos industriales, científicos y experimentales, y para aplicaciones médicas.

COMPUTER SYSTEMS
UNIT8: COMPUTERIZED NETWORK SYSTEMS

CFGS DAM
DPT INF

Estándares de la familia Wi-Fi

Estándar	Banda	Ancho de banda máximo
802.11a	5 GHz	54 Mbps
802.11b	2,4 GHz	11 Mbps
802.11g	2,4 GHz	54 Mbps
802.11n (Wi-Fi 4)	2,4 GHz y 5 GHz	600 Mbps
802.11ac (Wi-Fi 5)	5 GHz	7 Gbps
802.11ax (Wi-Fi 6)	2,4 GHz y 5 GHz	11 Gbps

1.3. Protocolo IPv4 e IPv6 (capa OSI red)

El protocolo IP, el más conocido del modelo TCP/IP, se encarga del enrutamiento o encaminamiento de paquetes de datos. Es decir, decide la ruta más adecuada para transportar los paquetes desde el origen al destino, pasando por diferentes nodos intermedios. Además, utilizará el direccionamiento a hosts (asignación de direcciones IP a interfaces de red) para poder enrutar los paquetes.

El protocolo IP no garantiza si un paquete llega a su destino y en qué orden, por lo que no es fiable, sin embargo, esta labor la pueden realizar otros protocolos de capas superiores como el protocolo TCP.

La dirección IP o dirección lógica se asigna a cada controlador o interfaz de red de un equipo que utilice el protocolo IP, como, por ejemplo, una tarjeta Wi-Fi o una tarjeta de Ethernet. Las direcciones IP son necesarias para enviar y recibir paquetes, identificando de forma unívoca cada dispositivo de red. Por tanto, no se pueden repetir dos direcciones IP en una misma red, ya que daría lugar a conflictos de red, ocasionando errores en la recepción o envío de datos.

Actualmente, se emplea el protocolo IP en sus versiones IPV4 e IPV6.

A) Protocolo IPv4

La versión IPv4 utiliza **32 bits**, desglosados en 4 bloques de 8 bits separados por puntos. De tal manera que cada bloque representa un número comprendido entre 0 y 255.

Además, el protocolo establece que se necesita una máscara de red, con el mismo formato que una dirección IP, asociada a la dirección IP. De esta manera, se identifica la red a la que pertenece la dirección IP.

COMPUTER SYSTEMS UNIT8: COMPUTERIZED NETWORK SYSTEMS

CFGS DAM
DPT INF

Intrínsecamente, la dirección IP se divide en una porción de red y una porción de host. La importancia de la máscara de red radica en que esta determina qué bits de la dirección IP se corresponden con la red a la que pertenece y qué bits especifica el host dentro de dicha red.

Un ejemplo de dirección IP y máscara de red asociada se muestra a continuación:



Ejemplo de dirección IP.



Ejemplo de máscara de red.

Los bits de la dirección IP que se encuentran en la misma posición que los bits 1 de la máscara de red (de izquierda a derecha) representan la porción de red. Y los bits de la dirección IP que se encuentran en la misma posición que los bits 0 de la máscara de red (de izquierda a derecha) representan la porción de host. Por ello, en el ejemplo anterior, los 3 primeros octetos (de izq. a derecha) de la dirección IP se corresponden con la dirección de red.

La máscara de red también se puede representar como sufijo, es decir, se indica la dirección IP y el número de unos que contiene la máscara de red intercalando el carácter "/" (conocida como **notación CIDR**). Por ejemplo, 192.168.0.1/24 equivale a indicar la dirección IP 192.168.0.1 con máscara de red 255.255.255.0.

El administrador de la red debe establecer las diferentes redes y el rango de direcciones IP dentro de cada una. Por tanto, antes de asignar la dirección IP y la máscara de red de cada adaptador o interfaz de red se ha de diseñar la organización lógica de la red mediante un **mapa de topología lógica** donde se especifiquen los dispositivos y el esquema de direccionamiento IP.

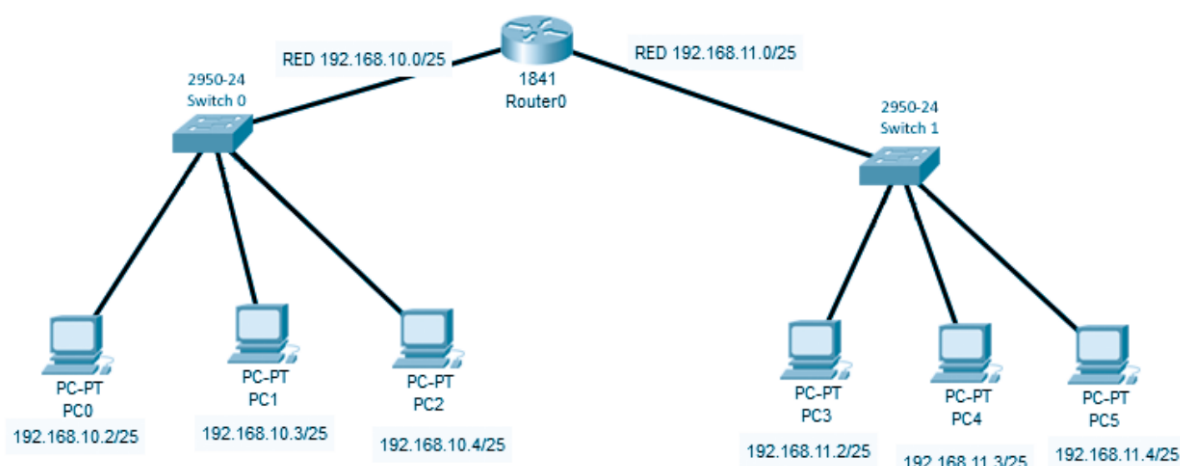
Dentro del rango de direcciones IP de cada red se diferencian varios tipos de direcciones, a saber:

- ✓ **Dirección de red:** especifica la red. Se identifica por la primera dirección del rango de direcciones de la red, es decir, todos los bits de la porción de host se encuentran a 0. Resulta equivalente a realizar una operación AND bit a bit entre la dirección IP y la máscara de red. Siguiendo con el ejemplo anterior, la dirección de red es: 192.168.0.0.
- ✓ **Dirección de broadcast:** empleada para enviar paquetes a todos los hosts de la red a la vez. Se identifica por la última dirección del rango de direcciones de la red, es decir, todos los bits de la porción de hosts se encuentran a 1. En el ejemplo, la dirección de broadcast sería: 192.168.0.255.

COMPUTER SYSTEMS UNIT8: COMPUTERIZED NETWORK SYSTEMS

CFGS DAM
DPT INF

- ✓ **Direcciones de hosts:** direcciones susceptibles de asignarse a hosts dentro de una red. Son aquellas comprendidas entre la dirección de red y la dirección de broadcast. En el ejemplo, la dirección mínima de host sería: 192.168.0.1 y la máxima 192.168.0.254.
- ✓ La **Puerta de enlace** es la dirección IP privada del equipo (o router) que se conecta a Internet mediante una dirección IP pública. Esta dirección IP es imprescindible para que pueda haber una conexión entre los demás equipos de la red y éste. Generalmente suele ser el primer host de la red. En el ejemplo sería 192.168.0.1.



Ejemplo de diseño lógico de una red

Las direcciones IP se pueden catalogar en:

- a) **Públicas:** para su uso con Internet y únicas a nivel mundial. Existen entidades que gestionan la asignación de direcciones IP públicas, como **IANA** (Assigned Numbers Authority) y los registros regionales de Internet, como el RIPE NCC en Europa.
- b) **Privadas:** designadas para redes con un acceso restringido o nulo con Internet. Solo los siguientes bloques de direcciones IP se pueden asignar a redes privadas y no son asignables para Internet.
 - 10.0.0.0/8
 - 172.16.0.0/12
 - 192.168.0.0/16

COMPUTER SYSTEMS
UNIT8: COMPUTERIZED NETWORK SYSTEMS

CFGS DAM
DPT INF

Private address range		
Class	start address	finish address
A	10.0.0.0	10.255.255.255
B	172.16.0.0	172.31.255.255
C	192.168.0.0	192.168.255.255

127.0.0.0 es loopback(eres t	Public address range		
	Class	start address	finish address
	A	0.0.0.0	126.255.255.255
	B	128.0.0.0	191.255.255.255
	C	192.0.0.0	223.255.255.255
	D	224.0.0.0	239.255.255.255
	E	240.0.0.0	254.255.255.255

Las redes privadas con acceso a Internet (como oficinas u hogares) disponen de un router que sí tiene acceso a Internet gracias al proveedor de servicios de Internet (compañía que da de alta el servicio). Este router es el que traduce direcciones IP privadas a públicas, y viceversa, gracias al **protocolo NAT**.

Además de la dirección lógica o dirección IP, los adaptadores de red disponen de una dirección física llamada **dirección MAC**, que está asociada a cada interfaz de red por el fabricante del producto. Esta dirección es única a nivel mundial y está formada por 48 bits que se representan de manera hexadecimal con un formato del tipo: XX-XX-XX-XX-XX-XX. Es empleada por la capa de enlace de datos del modelo OSI y gracias a ella el protocolo Ethernet establece origen y destino de cada trama.

-----ACTIVIDADES 1, 2 y 3 -----

B) Protocolo IPv6

El protocolo IP en su versión 6 (IPv6) emplea **128 bits** y se representa en hexadecimal en bloques de 2 bytes con un formato del tipo: 3D4A:1AD1:1FF0:43D1:A1BB:234C:4455:FF00.

COMPUTER SYSTEMS UNIT8: COMPUTERIZED NETWORK SYSTEMS	CFGS DAM DPT INF
-----------------------------------------------------------------------	-----------------------------------

Nota: El protocolo IPv6 presenta una serie de ventajas:

- Aumenta la seguridad en la comunicación
- Mejora el tratamiento de los paquetes
- Incrementa el número de direcciones IP asignables, de tal manera que prácticamente sean inagotables. Permite implantar el Internet de Todo (IoE).

Las direcciones IPv6 se pueden abreviar mediante las siguientes reglas:

1. El bloque 0000 se reduce a 0
2. Dos o más bloques consecutivos con valor 0 se reducen a "::" en una ocasión para una misma dirección.
3. Los ceros a la izquierda se pueden descartar
4. Ejemplo: la dirección 5560:0088:0000:0000:F103:31AA:75AC:0000 equivale a:
5560:88::F103:31AA:75AC:0

Además, una dirección IPv4, como, por ejemplo: 192.168.1.5, puede escribirse en notación IPv6 como 0:0:192:168.1.5, o también ::192.168.1.5.

-----ACTIVIDAD 4-----

1.4. Protocolo TCP y UDP (capa OSI transporte)

En la capa de transporte del modelo OSI los protocolos más empleados son el **protocolo de control de transmisión (TCP)** y el **protocolo de datagramas de usuario (UDP)**. Ambos se encargan de establecer comunicaciones entre aplicaciones de host de origen y de host de destino, enviando y recibiendo datos entre ellas sin importar las capas inferiores: medios de transmisión, rutas de los datos, congestiones, tipos de hosts, etc.

Con objeto de mantener conversaciones entre aplicaciones de origen y destino, ambos protocolos deben segmentar los datos en origen (dividiéndose en partes manejables llamados segmentos) y reconstruyéndolos en el destino. Además, a las aplicaciones que participan se les asigna un número de puerto exclusivo en cada host.

Los protocolos TCP y UDP se diferencian en la forma en que se transfieren los segmentos entre host.

- Protocolo TCP garantiza que todos los segmentos lleguen al destino. Para ello, realiza un seguimiento de todos los datos transmitidos y recibidos (el receptor envía un acuse de recibo). En caso de no recibir un segmento, este se vuelve a enviar. Por tanto, el protocolo TCP es confiable.

COMPUTER SYSTEMS
UNIT8: COMPUTERIZED NETWORK SYSTEMS

CFGS DAM
DPT INF

- Protocolo UDP envía segmentos entre aplicaciones de manera rápida sin importar su confiabilidad, ya que la pérdida de algunos segmentos no compromete la comunicación entre las aplicaciones.

El protocolo TCP es confiable, pero más lento que UDP, al realizar todo el proceso de seguimiento, acuse de recibo y retransmisión. Los protocolos FTP y HTTP emplean TCP, mientras que las aplicaciones de *streaming* de vídeo y audio suelen emplear UDP.

2. Configuración del protocolo TCP/IP

La asignación de una dirección IP a un adaptador de red puede realizarse de dos maneras: estática o dinámica.

2.1. Estática

Se emplea una **dirección IP fija para un host** (no cambia con el paso del tiempo), resultando ideal para servidores de Internet o que deban mantener la dirección IP para ofrecer servicios de impresión, HTTP, FTP, etc. La asignación de una dirección IP estática se puede realizar manualmente, por el administrador del sistema, a través de la configuración del adaptador de red.

Para configurar un adaptador de red Ethernet de manera estática en Windows lo hacemos a través de las “Conexiones de red”, pudiendo acceder a través de “Centro de redes y recursos compartidos” y “Cambiar opciones del adaptador”. Abrimos el adaptador Ethernet a configurar y accedemos a sus propiedades. Seleccionamos el “Protocolo de Internet versión 4 (TCP/IPv4)” y pulsamos en “Propiedades”.

El administrador de la red ha de indicarnos los datos de los campos para rellenar. Para lo que debemos habilitar la opción de “Usar la siguiente dirección IP”:

- ✓ Dirección IP
- ✓ Máscara de subred
- ✓ Puerta de enlace predeterminada o Gateway por defecto: normalmente es el router a través del cual accedemos a Internet. También puede ser otro host que interconecte redes distintas.

También debemos habilitar la opción “Usar las siguientes direcciones de servidor DNS”

COMPUTER SYSTEMS UNIT8: COMPUTERIZED NETWORK SYSTEMS

CFGS DAM
DPT INF

- Servidor DNS preferido: dirección IP de un servidor DNS que traduce direcciones de dominio a direcciones IP. Este servidor es el encargado, por ejemplo, de traducir el dominio <https://somgandia.com/> su dirección 188.114.96.5. Ejemplos de servidor DNS son Google Public DNS con IP 8.8.8.8 y 8.8.4.4 y OpenDNS con IP 208.67.222.222 y 208.67.220.220.
- DNS alternativo: es recomendable emplear otro servidor de DNS

Propiedades: Protocolo de Internet versión 4 (TCP/IPv4)

General

Puede hacer que la configuración IP se asigne automáticamente si la red es compatible con esta funcionalidad. De lo contrario, deberá consultar con el administrador de red cuál es la configuración IP apropiada.

☐ Obtener una dirección IP automáticamente

☒ Usar la siguiente dirección IP:

Dirección IP: 192 . 168 . 1 . 5

Máscara de subred: 255 . 255 . 255 . 0

Puerta de enlace predeterminada: 192 . 168 . 1 . 1

☐ Obtener la dirección del servidor DNS automáticamente

☒ Usar las siguientes direcciones de servidor DNS:

Servidor DNS preferido: 8 . 8 . 8 . 8

Servidor DNS alternativo: 208 . 67 . 222 . 222

☐ Validar configuración al salir

Opciones avanzadas...

Aceptar Cancelar

netplan-enp0s3

Cancelar Aplicar

Detalles Identidad IPv4 IPv6 Seguridad

Método IPv4

☐ Automático (DHCP) ☐ Sólo enlace local

☒ Manual ☐ Desactivar

☐ Compartida con otros equipos

Direcciones

Dirección	Máscara de red	Puerta de enlace
192.168.1.5	255.255.255.0	192.168.1.1

DNS Automático ☒

Direcciones IP separadas por comas

Para configurar un adaptador de red Ethernet de manera estática en Ubuntu, lo hacemos a través de "Red", desde "Configuración". Al pulsar en la rueda dentada del adaptador, accedemos a su configuración. En la pestaña IPv4 podemos introducir los datos de manera estática, seleccionando la opción "Manual".

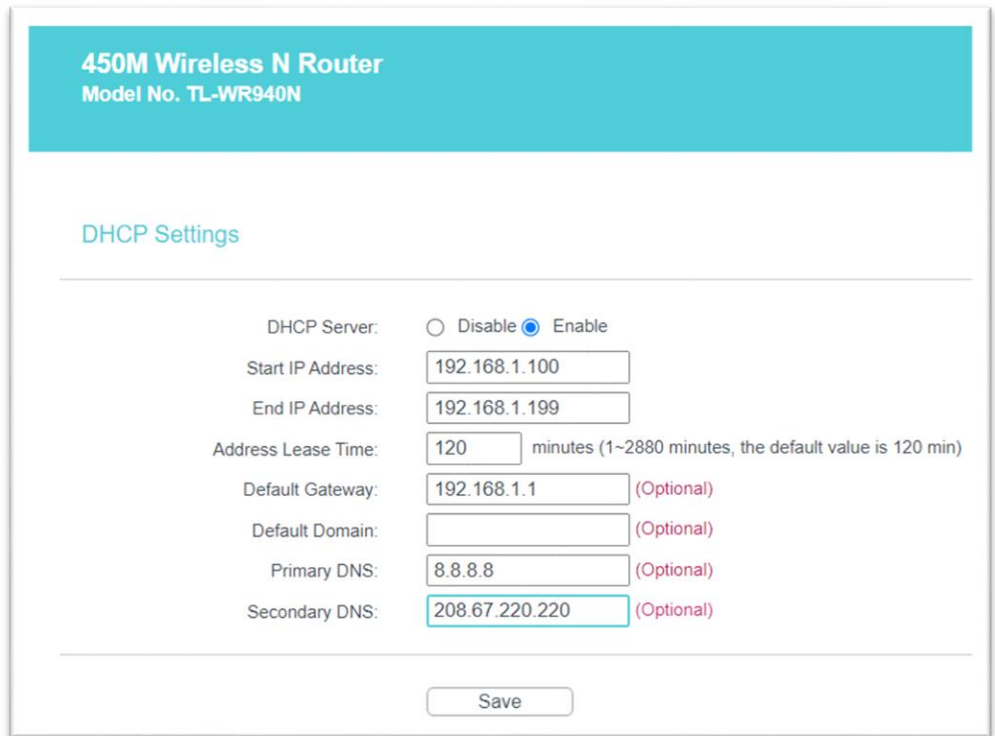
2.2. Dinámica

Con este mecanismo, la dirección IP cambia con el paso del tiempo. La mayoría de los equipos emplean este método gracias al **protocolo DHCP**. Dicho protocolo emplea un servidor DHCP, que provee la configuración necesaria a los clientes DHCP (hosts con esta configuración del adaptador de red habilitada) para poder comunicarse en red: dirección IP, máscara de red, servidor DNS, puerta de enlace, etc. Los **routers SoHo** (Small office Home office), es decir, los que solemos tener en casa u oficinas, habilitan este servidor por defecto y, por tanto, no nos tenemos que preocupar de su configuración.

COMPUTER SYSTEMS
UNIT8: COMPUTERIZED NETWORK SYSTEMS

CFGS DAM
DPT INF

Los servidores DHCP permiten establecer el rango de direcciones asignables por este protocolo. El resto de direcciones IP se reservan para direccionamiento estático. En la siguiente imagen se aprecia la configuración del servidor DHCP de un router SoHo, donde se indica el rango de direcciones IP asignadas por DHCP (dirección IP de inicio y fin), direcciones de servidores DNS, Gateway por defecto, etc. Todos estos datos se trasladan a la configuración TCP/IP de los clientes DHCP.



450M Wireless N Router
Model No. TL-WR940N

DHCP Settings

DHCP Server: ☐ Disable ☒ Enable

Start IP Address:

End IP Address:

Address Lease Time: minutes (1~2880 minutes, the default value is 120 min)

Default Gateway: (Optional)

Default Domain: (Optional)

Primary DNS: (Optional)

Secondary DNS: (Optional)

Por tanto, la configuración de las propiedades del Protocolo de Internet versión 4 (TCP/IPv4) se ha de mantener en automático para obtener una dirección IP dinámica.

Puedes hacer pruebas de configuración de routers en el siguiente link: <https://www.tp-link.com/es/support/emulator/> (login: admin)

ACTIVIDAD 5 y 6

3. Interconexión de redes. Componentes

Los sistemas informáticos en red emplean dispositivos intermedios que conectan distintas redes y host entre sí. Estos elementos se clasifican según la capa del modelo OSI sobre la que actúan.

COMPUTER SYSTEMS UNIT8: COMPUTERIZED NETWORK SYSTEMS

CFGS DAM
DPT INF

Dispositivos de interconexión por capas

Capa	Dispositivo	Función
Física	Repetidor	Regenera la señal entre dos puntos de una red. Existen inalámbricos o cableados.
	Hub	Replica la información entrante por uno de sus puertos al resto de puertos.
Enlace de datos	Switch	Conecta la información entrante por uno de sus puertos al puerto de destino únicamente.
	Punto de acceso	Extiende la red cableada mediante un medio inalámbrico. Pertenecer a las capas 1 y 2 del modelo OSI.
Red	Router	Conecta redes diferentes.

3.1. Switch (capa OSI enlace de datos)

Trabaja en la capa de enlace de datos del modelo OSI y tiene como función conectar varios segmentos de una misma red o, lo que es equivalente, dividir una red en subredes.

El switch, a diferencia del hub, evita que colisionen paquetes de datos en el medio de transmisión. Para ello, cuando un paquete es recibido por uno de sus puertos, solo lo retransmitirá al puerto de destino y no a todos los restantes.



3.2. Router. Tablas de enrutamiento (capa OSI red)

El router pertenece a la capa de red del modelo OSI y se encarga de conectar diferentes redes. Son dispositivos que disponen de su propio sistema operativo, CPU, RAM y ROM.



Existen dos tipos de routers:

- **Rackable o empresarial:** empleados para la conectividad en armarios o racks donde se necesitan unas prestaciones superiores.

COMPUTER SYSTEMS UNIT8: COMPUTERIZED NETWORK SYSTEMS

CFGS DAM
DPT INF

- **Routers SoHo:** son los que suelen suministrar los proveedores de acceso a Internet. Estos permiten conectar la red local de nuestra casa con Internet. Integran otros dispositivos como: switch, punto de acceso Wi-Fi y firewall.



Router SoHo Netgear.

Tanto los routers como los hosts utilizan las tablas de enrutamiento para encaminar los paquetes a otros dispositivos de una red local o remota. Cuando dos hosts se encuentran en una misma red local, en su comunicación no interviene el router. Sin embargo, cuando la comunicación es remota (redes distintas) entre un host origen y otro destino, sí son necesarios.

Los hosts emplean tablas de enrutamiento que almacenan las direcciones de hosts a los que pueden enviar paquetes, que pueden ser:

- ✓ A él mismo. Se suele utilizar para realizar pruebas (IP 127.0.0.0/8).
- ✓ A un host local
- ✓ A un host remoto. Cuando no encuentra una coincidencia en la tabla de enrutamiento, se entiende que es un host remoto y utiliza la dirección por defecto 0.0.0.0, que indica la puerta de enlace que se hará cargo del paquete.

Podemos observar la tabla de enrutamiento de un host en Windows con el comando **netstat -r** y en GNU/Linux con **ip route show**.

Los routers emplean tablas de enrutamiento más complejas para poder enviar paquetes a redes diferentes, localizando la ruta más conveniente. Estas tablas se almacenan en la memoria de los routers. En ellas se indican las redes de destino, la métrica (valor asociado a cada destino que discrimina un mejor o peor encaminamiento) y la interfaz de salida para alcanzar la red de destino.

Los routers disponen de tres tipos de entradas en sus tablas de enrutamiento:

- Conexiones locales. Conectadas directamente por alguna interfaz del router
- Conexiones estáticas. Establecidas manualmente por el administrador de la red
- Conexiones dinámicas. Entradas que han sido aprendidas mediante algún algoritmo de enrutamiento. Estos algoritmos son utilizados por los routers para comunicarse e intercambiar entradas entre ellos. La mayoría de las entradas son de este tipo.

COMPUTER SYSTEMS UNIT8: COMPUTERIZED NETWORK SYSTEMS

CFGS DAM
DPT INF

3.3. Topología física y lógica. Mapas

El diseño de una red de computadores se realiza mediante mapas que establecen la organización física o lógica de los dispositivos o componentes implicados. De esta manera, se estudia la organización de cara a su implementación y mejorar su eficiencia, según los objetivos que se pretendan conseguir. Así pues, distinguimos entre:

A) Topología física

Ilustra la organización de los componentes y conexiones físicas entre elementos de red. Dentro de las topologías físicas, distinguimos los siguientes tipos:

- ✓ Inalámbricas:
 - Distribuida: se emplean puntos de acceso para que los clientes se conecten a la red y se puedan mover libremente, saltando de uno a otro de forma transparente para ellos.
 - Centralizada: se utilizan puntos de acceso sin capacidad de gestión, ya que se conectan varios de ellos a switches WLAN. Estos son los encargados de realizar el control y la gestión de la red Wi-Fi.
- ✓ Cableadas:
 - Redes de área extensa (WAN):
 - Punto a punto: 2 equipos se comunican directamente
 - Estrella: un equipo central interconecta todos los dispositivos
 - Malla: todos los equipos están interconectados entre sí parcialmente o totalmente.
 - Redes de área local (LAN):
 - Estrella
 - Estrella extendida: estrellas unidas entre sí
 - Bus: un medio totalmente compartido al cual se conectan distintos equipos
 - Anillo: un medio compartido cerrado donde se conectan los equipos.



Topología
de bus



Topología
de anillo



Topología
en estrella



Topología
en estrella extendida



Topología
en malla

Topologías cableadas.

COMPUTER SYSTEMS UNIT8: COMPUTERIZED NETWORK SYSTEMS

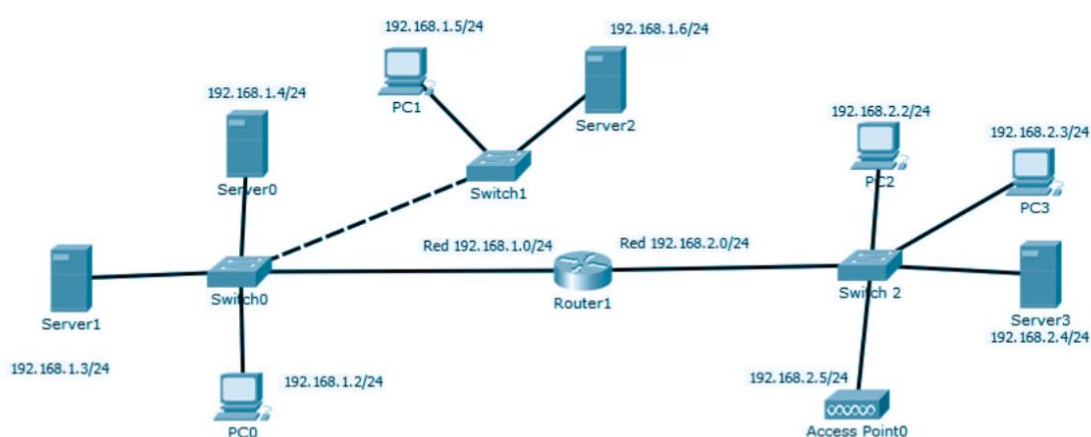
CFGS DAM
DPT INF

B) Topología lógica

Para cada elemento de red se establece su configuración para la comunicación y acceso al medio. Dentro de las topologías lógicas, distinguimos los siguientes tipos:

- En redes WAN: se considera una conexión punto a punto entre 2 equipos.
- En redes LAN: tenemos un medio compartido, con lo cual se necesita un conjunto de reglas para controlar el acceso. Para ello, existen 2 métodos:
 - Acceso por contienda: cuando un equipo desea enviar al medio una trama hacia otro equipo, este escucha el medio y, si está libre, la envía. Si durante la transmisión se produce una colisión (dos tramas se interceptan al ser enviadas a la vez), la trama se descarta y se espera un tiempo para volver a enviarla. Empleado en redes Ethernet y Wi-Fi a través de los mecanismos CSMA/CD y CSMA/CA.
 - Acceso controlado: se establece un turno para poder enviar una trama. Cuando le toca el turno a un equipo, este puede enviar la trama. Si no lo hace, debe esperar a que le toque su turno. Este tipo de métodos es común en redes físicas en anillo, como Token Ring o FDDI.

A continuación, se muestra un mapa lógico en el que intervienen diferentes elementos de red. Podemos distinguir los nombres de cada equipo de red, su dirección IP y líneas de conexión con otros dispositivos.



Ejemplo de mapa lógico.

En la imagen superior podemos distinguir 2 redes distintas, las cuales se comunican a través del router. Los switches comunican segmentos de una misma red.

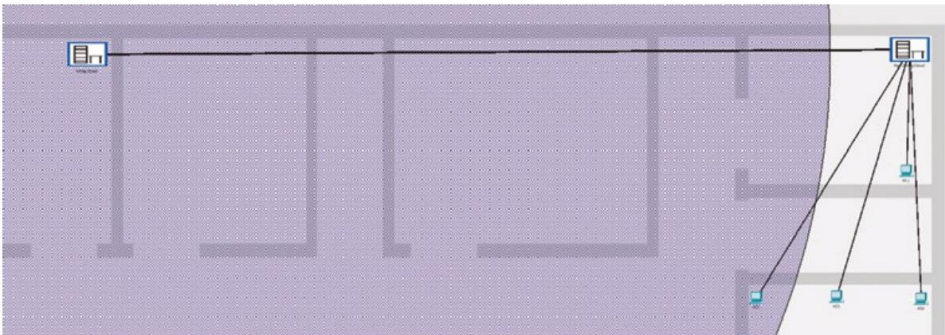
COMPUTER SYSTEMS UNIT8: COMPUTERIZED NETWORK SYSTEMS

CFGS DAM
DPT INF

Nota: En un mapa lógico, la dirección IP de los elementos es fundamental para la comprensión de la organización.

A continuación, mostramos el mapa físico correspondiente al mapa lógico anterior. Distinguimos las estancias, los computadores de la red, los armarios de distribución y el rango de cobertura Wi-Fi en color púrpura en el punto de acceso. Los componentes de red, como servidores, switches y routers se encuentran en los racks.

Ejemplo de mapa físico



3.4. Dominios de colisión y difusión

Los dispositivos de capa 2 o superiores, como los routers y switches, dividen los dominios de colisión (áreas donde pueden colisionar paquetes). Además, los dispositivos de capa 3 o superiores, como los routers, dividen los dominios de difusión (áreas donde se reciben tramas de broadcast).

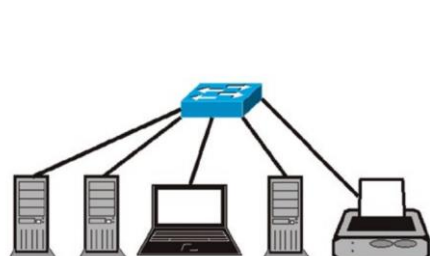
La segmentación de una red de colisión y dominios de difusión mejora la eficiencia de la red y aumenta el ancho de banda.

Ejemplos:

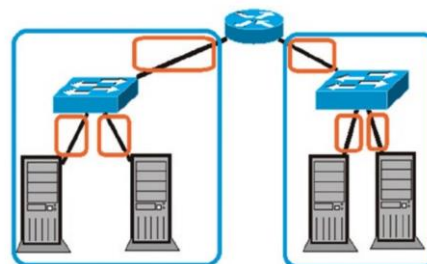
A continuación, en la primera imagen se distinguen 5 dominios de colisión, uno para cada dispositivo conectado al switch. En la imagen siguiente se muestran 2 dominios de difusión (en azul) que, a su vez, disponen de 3 dominios de colisión cada uno (en naranja).

COMPUTER SYSTEMS UNIT8: COMPUTERIZED NETWORK SYSTEMS

CFGS DAM
DPT INF



Dominios de colisión.



Dominios de colisión.

4. Tipos de redes

Las redes se pueden clasificar atendiendo a diferentes criterios:

A) Según su tamaño:

- Redes de área personal (PAN): su ámbito de acción es el entorno del propio usuario. Emplean tecnologías como Bluetooth, Zigbee o NFC.
- Redes de área local (LAN). Una red LAN inalámbrica se conoce como WLAN (Wireless LAN)
- Redes de área metropolitana (MAN): redes de extensión intermedia entre LAN y WAN, que suelen estar constituidas por varias redes LAN. Ejemplo de ello son las conexiones entre poblaciones próximas o el entorno de un campus universitario. Una red MAN inalámbrica se conoce como WMAN (Wireless MAN).
- Redes de área extensa (WAN): redes de larga distancia que conectan redes LAN o WAN. Las redes WAN pueden conectar ciudades lejanas e incluso continentes.

B) Según su transmisión:

- Redes punto a punto: se transmite la información desde un host origen a un host destino a través de un medio.
- Redes multipunto: permite transmitir la información desde un host a múltiples destinos compartiendo el mismo medio.

C) Según su función:

- Redes entre iguales: los hosts interconectados ofrecen y acceden por igual a los servicios.
- Redes cliente-servidor: unos hosts ofrecen servicios y recursos (servidores) y otros acceden a ellos (clientes).

COMPUTER SYSTEMS UNIT8: COMPUTERIZED NETWORK SYSTEMS	CFGS DAM DPT INF
-----------------------------------------------------------------------	-----------------------------------

D) Según los medios empleados:

- Inalámbricas: emplean ondas electromagnéticas para la transmisión de información por el aire. Existen muchos estándares inalámbricos, siendo los más conocidos Bluetooth y Wi-Fi.
- Cableada: utilizan algún medio físico para transmitir señales portadoras de información. Los medios más empleados son el cable de par trenzado de cobre y el cable de fibra óptica de vidrio o plástico.
- Mixtas: utilizan ambos medios.

5. Acceso a redes WAN. Tecnologías

Cuando se necesita comunicar varias redes LAN entre sí a largas distancias, entran en acción las redes WAN. Las redes LAN son propiedad de particulares que, cuando deciden conectarse a otra red LAN inalcanzable geográficamente por dicho propietario o a Internet, deben suscribirse a un proveedor de servicios de red o un proveedor de Internet (ISP).

Las redes de área extensa requieren estándares y tecnologías diferentes a las redes LAN debido a las grandes distancias con las que trabajan. Principalmente, estas tecnologías se centran en las capas de red, enlace de datos y física del modelo OSI.

Las principales tecnologías WAN se agrupan en diferentes tipos de conexión:

5.1. Conexiones WAN privadas

Entre las conexiones privadas, se pueden encontrar diversos tipos:

COMPUTER SYSTEMS UNIT8: COMPUTERIZED NETWORK SYSTEMS

CFGS DAM
DPT INF

- ✓ **Conmutación de circuitos:** requieren que se establezca un circuito (canal) dedicado entre los nodos y terminales antes de que se comuniquen los usuarios. Ejemplo de ello es la red telefónica conmutada tradicional, donde el canal es compartido por varias conversaciones gracias a la multiplexación por división temporal (TDM), la cual reparte el tiempo de las conexiones por turnos. Ejemplos de tecnologías de este tipo son PSTN e ISDN (RDSI).
- ✓ **Conmutación de paquetes:** divide los datos para transmitir en paquetes a través de una red compartida. A diferencia de la conmutación de circuitos, no es necesario que se establezca un circuito previamente. Además, la red compartida facilita la comunicación entre multitud de pares de nodos a través del mismo canal. Por ello, este tipo de conexión WAN resulta más económica que la conmutación de circuitos, aunque sus latencias son superiores. No obstante, las tecnologías actuales de este tipo permiten comunicaciones de voz y vídeo. Ejemplos son Frame Relay, x.25 y ATM.

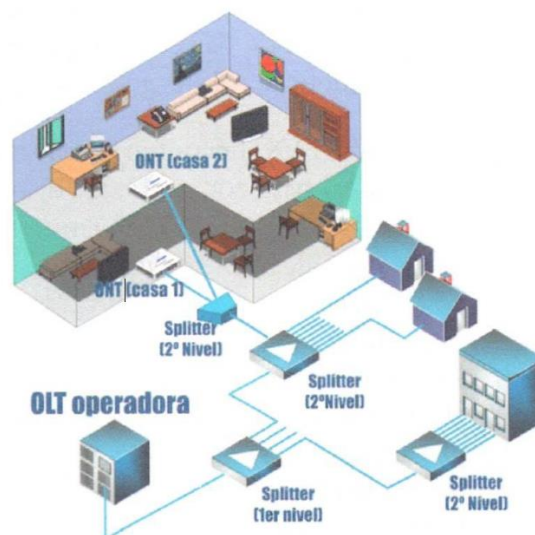


Figura 5.16
Elementos de conexión FTTH.

Fuente: <http://fibraopticahastaelhogarecuador>.

- ✓ **Dedicada:** se emplea para una conexión directa y permanente entre 2 nodos de la red WAN del proveedor de servicios (conectando diferentes localizaciones del cliente entre un origen y un destino remoto). Su coste es muy elevado, pero se reducen tiempos de latencia, siendo ideal para voz sobre IP (VoIP) y vídeo sobre IP.

5.2. Conexiones WAN públicas

A continuación, se detallan las conexiones WAN públicas más usadas:

- **DSL (Digital Subscriber Line):** es una familia de tecnologías, como SDL, IDSL, HDSL, VDSL y ADSL, en sus diferentes versiones. Permiten acceder a Internet mediante cables de cobre de par trenzado de la red telefónica con un ancho de banda aceptable.

COMPUTER SYSTEMS
UNIT8: COMPUTERIZED NETWORK SYSTEMS

CFGS DAM
DPT INF

- ~~FTTH~~ e fibra hasta el hogar: alcanza velocidades muy superiores a la familia DSL, empleando fibra óptica desde la red troncal hasta los clientes. ~~Utilizan un conjunto de equipos con tecnología GPON (Gigabit-capable Passive Optical Network), a saber:~~
 - ~~OLT (Optical Line Termination): dispositivo activo del que parten las fibras a los diferentes usuarios.~~
 - ~~Divisor óptico o splitter: divide la señal óptica entrante en partes iguales de menor potencia a diferentes ramas o usuarios. Existen splitters de diferentes niveles de división, según la envergadura de la red troncal, y de distribución.~~
 - ~~ONT (Optical Network Terminal): convierte las señales ópticas en señales eléctricas, y viceversa. Se integra en los routers SoHo actualmente.~~
- ~~HFC~~ e híbrido fibra-coaxial: emplea fibra óptica en la red troncal y cable coaxial en su red de distribución hasta los hogares.
- Inalámbricas: existen diferentes tecnologías que utilizan ondas electromagnéticas para la transmisión de datos. ~~Principalmente, se diferencian en la longitud de onda empleada y su frecuencia, por lo que son muy empleadas en redes WAN:~~
 - ~~WiMAX: permiten un alcance alrededor de 60 km, pudiendo alcanzar 1 Gbps. Es ideal para zonas que no dispongan de cobertura por cable.~~
 - ~~LTE-A (4G) y 5G: permiten gran movilidad de los terminales inalámbricos, llegando a alcanzar varios Gbps.~~

Nota: Internet se emplea como una alternativa muy económica al uso de conexiones WAN privadas. Ejemplo de ello es la tecnología VPN (Virtual Private Network), ya que permite establecer una conexión segura a través de una red pública (como Internet) entre redes privadas.

6. Redes cableadas

Las redes de comunicación cableadas son aquellas que emplean algún medio de transmisión guiado, como cables de cobre (coaxial o par trenzado) o de fibra óptica. Aunque la instalación de los medios guiados es mucho más compleja que los inalámbricos, presentan multitud de ventajas, como su seguridad o un ancho de banda sostenido.

6.1. Tipos y características

Los medios de transmisión cableados más utilizados son el cable de cobre de par trenzado y la fibra óptica, los cuales detallamos a continuación:

COMPUTER SYSTEMS UNIT8: COMPUTERIZED NETWORK SYSTEMS

CFGS DAM
DPT INF

A) Cable de cobre par trenzado

Formado externamente por una cubierta de PVC, que dispone en su interior de 8 cables aislados y entrelazados, identificados por el color individual de su cubierta. Los cables están entrelazados por pares de la siguiente manera:

- ✓ Azul — blanco/azul
- ✓ Naranja — blanco/naranja
- ✓ Verde — blanco/verde
- ✓ Marrón — blanco/marrón



Cable UTP (sin blindaje).

Podemos encontrar protegido el cable contra interferencias electromagnéticas externas mediante diferentes blindajes en los pares o en el cable.

Tipos de blindajes en cable de cobre de par trenzado		
U/FTP	Pantalla de aluminio en los pares	
F/FTP	Pantalla de aluminio en los pares y en el cable	
S/FTP	Pantalla de aluminio en los pares y malla de aluminio en el cable	
F/UTP	Pantalla de aluminio en el cable	
SF/UTP	Pantalla y malla de aluminio en el cable	

Además, los cables emplean conectores de tipo RJ-45 para su conexión en tarjetas adaptadoras de red, routers, switches, etc. Este conector presenta la siguiente forma.

COMPUTER SYSTEMS UNIT8: COMPUTERIZED NETWORK SYSTEMS

CFGS DAM
DPT INF



La terminación de los cables en el conector, es decir, el orden en el que han de ser engastados a él, está regulada por la norma TIA/EIA-568-B, la cual establece dos tipos: T-568A y T-568B. El orden de cada terminación es el siguiente:

- T-568A:

1. Blanco/verde
2. Verde
3. Blanco/naranja
4. Azul
5. Blanco/azul.
6. Naranja
7. Blanco/marrón
8. Marrón

- T-568B

1. Blanco/naranja
2. Naranja
3. Blanco/verde
4. Azul
5. Blanco/azul.
6. Verde
7. Blanco/marrón
8. Marrón

El cable con la misma terminación en ambos extremos se denomina directo, y con distinta terminación, cruzado.

Además, el estándar TIA/EIA-568B determina varias categorías de cable de par trenzado, según sus características eléctricas. Esto detalla aspectos, como su frecuencia de funcionamiento y la velocidad máxima. Las más utilizadas son: Cat5e, Cat6, Cat6a, Cat7, Cat7a y Cat8. A mayor categoría, mayor es su frecuencia y ancho de banda.



El cable de cobre de par trenzado destaca por su facilidad en la instalación, prestando un gran ancho de banda a un bajo coste, tanto en el propio medio como en los dispositivos de interconexión.

-----ACTIVIDAD 7-----

COMPUTER SYSTEMS UNIT8: COMPUTERIZED NETWORK SYSTEMS

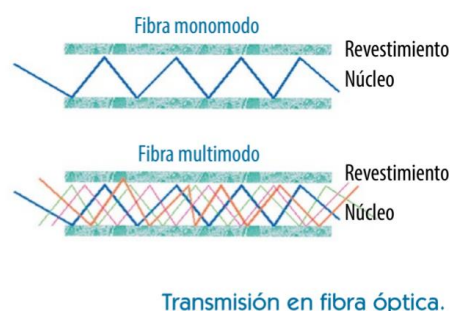
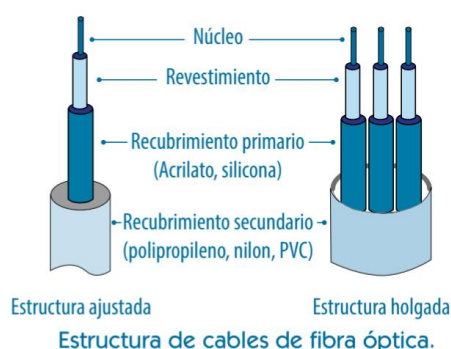
CFGS DAM
DPT INF

B) Cable de fibra óptica

El cable de fibra óptica está formado por uno o más hilos de fibra de vidrio o plástico, recubierto por varias capas de diferentes materiales para dotarle de protección y rigidez.

Podemos clasificar los cables de fibra óptica en diferentes tipos:

- ✓ Según su estructura interna
 - Estructura holgada: los hilos de fibra óptica se encuentran con cierta libertad en tubos dentro del cable de fibra óptica. Es utilizada principalmente en redes de área local (LAN) y metropolitanas (MAN)
 - Estructura ajustada: los hilos de fibra óptica no presentan libertad de movimientos debido a su recubrimiento secundario, por lo que solo existe un hilo de fibra por tubo. Normalmente se emplea para redes metropolitanas (MAN) y de área extensa (WAN).
- ✓ Según el modo de transmisión
 - Monomodo (SM): se emite un único haz de luz por el interior del hilo. Es empleado principalmente para largas distancias. Los estándares monomodo más utilizados son OS1 y OS2.
 - Multimodo (MM): transmite varios haces de luz con diferentes trayectorias. Se suele utilizar para distancias cortas (entre manzanas de edificios o en el interior de estos). Los estándares más empleados son OM1, OM2, OM3, OM4 y OM5.



COMPUTER SYSTEMS UNIT8: COMPUTERIZED NETWORK SYSTEMS

CFGS DAM
DPT INF



Conector LC.



Conector SC.



Conector MT-RJ.



Conector MPO.

Nota: A diferencia de los cables de cobre de par trenzado, los cables de fibra óptica son extremadamente seguros en su transmisión y son capaces de sostener velocidades muy altas a larga distancia. Sin embargo, en su despliegue e instalación se requieren dispositivos caros (como fusionadoras de fibra óptica), así como elementos de interconexión de coste superior a los de cobre de par trenzado.

-----ACTIVIDAD 8-----

6.2. Dispositivos de interconexión

El estándar TIA/EIA 568-B, que define el diseño e implementación del cableado en un edificio o entre varios, establece una topología de red en estrella. En la topología en estrella, los nodos y hosts están conectados a un nodo central que conmuta y controla el flujo de datos entre todos ellos.

Los elementos de electrónica de red empleados para conectar cables de par trenzado como nodo central son principalmente los switches y routers. Estos dispositivos se instalan en armarios de distribución o racks, que alojan multitud de elementos, dependiendo de la envergadura de la infraestructura de red. Los racks suelen contener:

- **Dispositivos de electrónica de red:** switches, routers, etc.
- **Paneles de parcheo (patch panel):** elementos de conexión de cables que facilitan la conexión, organización y estructura del cableado en el rack. En el otro extremo del cable, la terminación es la toma de usuario en las áreas de trabajo.
- **Otros elementos:** regletas eléctricas, bandejas, organizadores de cables, etc. También existen dispositivos de interconexión y adaptadores de red de fibra óptica y mixtos (para cables de par trenzado y fibra óptica).

También existen dispositivos de interconexión y adaptadores de red de fibra óptica y mixtos (para cables de par trenzado y fibra óptica).

COMPUTER SYSTEMS UNIT8: COMPUTERIZED NETWORK SYSTEMS

CFGS DAM
DPT INF



Detalle de un rack.

-----ACTIVIDAD 9 -----

6.3. Adaptadores

Las tarjetas de red o adaptadores de red, también llamados NIC (Network Interfaz Controller), son necesarios para que los hosts puedan conectarse a una red. Existen diferentes tipos, atendiendo de las características de estas:



Roseta con cuatro tomas.

- a) Medio de transmisión: cable de cobre de par trenzado, fibra óptica, etc.
- b) Conectividad con el host: integrada, PCIe, USB, etc.
- c) Modo de transmisión: full dúplex o half dúplex, según pueda emitir y recibir datos de forma simultánea o no, respectivamente.
- d) Velocidad de conexión: 10Mbps, 100Mbps, 1Gbps, 10Gbps, etc.
- e) Wake On LAN: características que permite el adaptador encender el host de forma remota.



Tarjeta de red con puerto RJ-45.

COMPUTER SYSTEMS
UNIT8: COMPUTERIZED NETWORK SYSTEMS

CFGS DAM
DPT INF

7. Redes inalámbricas

Las redes inalámbricas aportan ventajas con respecto a las redes cableadas, como la movilidad, la flexibilidad y la facilidad de instalación. Estas emplean ondas electromagnéticas para transmitir datos, cuya capacidad de transmisión depende, principalmente, de:

- ✓ ~~Longitud de onda: distancia entre 2 crestas o valles consecutivos de una onda. Se mide en metros~~
- ✓ ~~Frecuencia: número de veces que se repite una onda en un segundo. Se mide en hercios (Hz).~~

~~El espectro electromagnético representa un amplio rango de ondas electromagnética, según su longitud de onda.~~

7.1. Tipos y características

Las redes inalámbricas más usadas son las redes Wi-Fi, WiMAX, los sistemas de comunicación móviles 4G y 5G, así como otras redes WPAN, como Bluetooth o Zigbee.

Cada una dispone de unas características que las hacen más apropiadas para según qué aplicaciones o usos. Pero dichas características pueden reducir su capacidad de transmisión debido a factores, como colapso de la banda de trabajo de la red inalámbrica, fuentes electromagnéticas externas, número de usuarios conectados, posicionamiento de las antenas y de los receptores, uso en interiores o exteriores, etc.

A) Wi-Fi

Su principal objetivo es la transmisión de datos a gran velocidad en una red local. Wi-Fi se basa en el conjunto de estándares IEEE 802.11, ~~entre los que destacamos: IEEE 802.11b, IEEE 802.11g, IEEE 802.11n y 802.11ac (Wi-Fi 5).~~

Estos estándares trabajan en las bandas de 2,4 Hz y 5 GHz, pudiendo alcanzar un ancho de banda teórico de 10 Gbps con un alcance de 1Km, aproximadamente. Cada estándar posee un rango de acción y ancho de banda diferente que está asociado a su frecuencia. A menor frecuencia, mayor es su alcance y menor ancho de banda.

Estas redes necesitan puntos de acceso Wi-Fi para conectar los diferentes terminales con NIC inalámbricas como teléfonos inteligentes, computadores, Smart TV, etc.

ACTIVIDAD 10

COMPUTER SYSTEMS UNIT8: COMPUTERIZED NETWORK SYSTEMS	CFGS DAM DPT INF
-----------------------------------------------------------------------	-----------------------------------

B) WiMAX

Establece una red de comunicación de alta velocidad para redes MAN ~~con alcance de decenas de kilómetros. Se fundamenta en la familia de estándares IEEE 802.16, llegando a alcanzar 1 Gbps.~~

Su infraestructura es parecida a los sistemas de comunicación móvil 4G y 5G. Requieren estaciones base con dispositivos electrónicos para emitir señales microondas y receptores WiMAX.

Nota: Debido a sus características y el coste de instalación, su aplicación se centra en dotar de acceso a Internet y telefónico a áreas geográficas poco densas o lejanas, donde el coste del despliegue de cable de fibra óptica o de cobre resultaría costoso.

C) Sistemas de comunicación móvil 4G y 5G

Las siglas 4G y 5G hacen mención a las actuales generaciones de tecnologías de comunicación móvil para redes WMAN y WWAN.

El estándar LTE-Advanced detalla las características técnicas de la 4ª generación con un ancho de banda de hasta 1 Gbps.

~~El estándar 5G NR recoge los aspectos técnicos de la generación 5G, pudiendo alcanzar 20 Gbps. Su consumo es muy inferior a su antecesor y presenta mayor capacidad, siendo ideal para aplicaciones en tiempo real y el desarrollo del IoT (Internet de las Cosas).~~

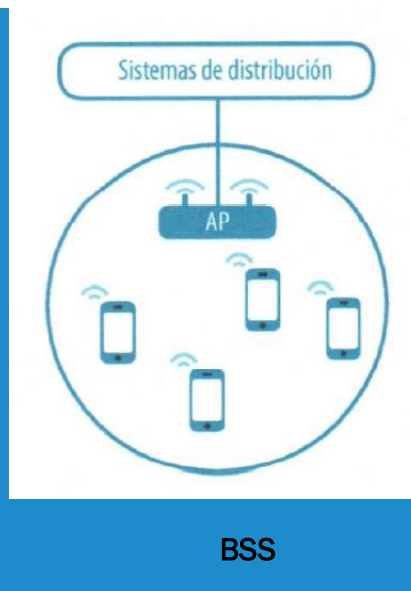
D) Otras redes WPAN

Además, se suelen utilizar redes de área personal inalámbricas para una comunicación entre dispositivos de forma directa, sin utilizar dispositivos intermedios. Los más empleados son:

COMPUTER SYSTEMS UNIT8: COMPUTERIZED NETWORK SYSTEMS

CFGS DAM
DPT INF

- Zigbee: definido por el estándar IEEE 802.15.4, que se fundamenta en su bajo consumo y baja transferencia de datos. Sus principales usos son aplicaciones de control y monitorización a muy bajo coste.
- Bluetooth: recogido en el estándar IEEE 802.15.1, pretende facilitar transmisión de datos y voz entre dispositivos cercanos, así como la sincronización, eliminando su conexión por medio de cables. Su empleo en condiciones ideales puede superar los 200m y un ancho de banda de varias decenas de bps.



Tanto Zigbee como Bluetooth, en sus diferentes versiones, se orientan cada vez más al IoT, gracias a la reducción del consumo, bajo coste y mayor rango de acción.

Además, existen otros estándares, como NFC, que se consideran de corto alcance y permiten una comunicación de datos entre 2 dispositivos a pocos cms de distancia.

7.2. Dispositivos de interconexión

Cada tipo de red inalámbrica requiere dispositivos de interconexión adecuados a las características de transmisión definidas por el estándar de dicha red. Se crea así la infraestructura de red inalámbrica necesaria en cada caso.

De esta manera, en redes WiMAX, 4G o 5G, las estaciones base están provistas de equipos de telecomunicaciones y antenas que aportan la cobertura necesaria a los usuarios de una zona.

En el caso de la tecnología Wi-Fi, normalmente se utilizan puntos de acceso Wi-Fi (PA) para conectarse y ofrecer los servicios necesarios a los distintos dispositivos, creando así la red inalámbrica. No obstante, se pueden utilizar diferentes topologías de red:

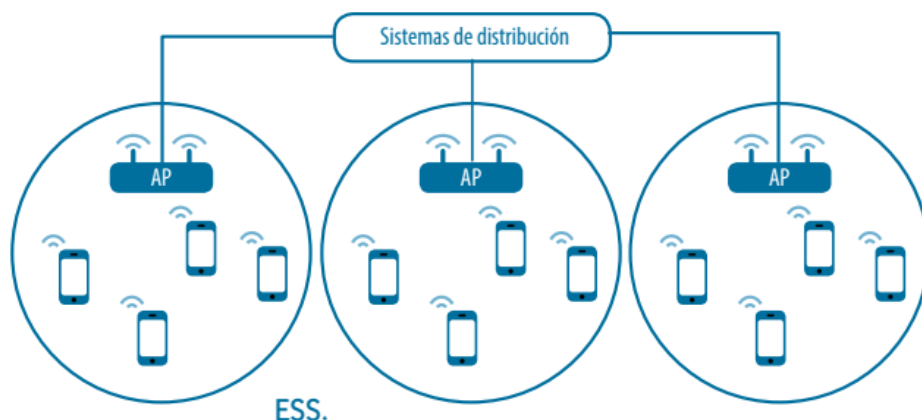
- a) Modo ad hoc (~~IBSS~~): 2 clientes se conectan directamente sin emplear ningún dispositivo de infraestructura.

COMPUTER SYSTEMS UNIT8: COMPUTERIZED NETWORK SYSTEMS

CFGS DAM
DPT INF

b) Modo infraestructura: los clientes se conectan mediante un dispositivo de infraestructura (normalmente puntos de acceso inalámbricos). Estos puntos de acceso Wi-Fi se conectan al sistema de distribución (normalmente switches o routers). Diferencia 2 tipos:

- ~~Conjunto de servicios básicos (BSS): existe un único punto de acceso que ofrece unos servicios básicos para que los clientes se puedan comunicar en la zona de cobertura de dicho punto de acceso. Si los clientes se salen de la zona de cobertura, no se podrán comunicar.~~
- ~~Conjunto de servicios extendidos (ESS): varios puntos de acceso se conectan mediante un sistema de distribución (De manera cableada o inalámbrica). Gracias a ello, se amplía la zona de cobertura y los clientes pueden circular entre puntos de acceso sin perder la conexión.~~



En general, los estándares Bluetooth y NFC trabajan en modo ad hoc, mientras que Zigbee puede trabajar en ambos modos de infraestructura.

7.3. Adaptadores

Los equipos que deseen conectarse a una red inalámbrica necesitan adaptadores de red inalámbricos del tipo de red a la que va a conectarse. Muchos de ellos integran estos adaptadores en el propio hardware de los dispositivos, como los smartphones (que integran adaptadores Wi-Fi, 4G, 5G, Bluetooth, NFC, etc.), los portátiles y placas base de computadores de sobremesa que integran (adaptadores Ethernet, Bluetooth o Wi-Fi). En otros casos, podemos adquirir adaptadores inalámbricos externos o internos, que deben instalarse en alguna ranura de expansión interna o puerto de conexión externo.

Las características más importantes de los adaptadores de red Wi-Fi son:

- ✓ Estándares Wi-Fi soportados: los más comunes son IEEE 802.11 a/b/g/n/ac.
- ✓ Bandas de trabajo (frecuencias)

COMPUTER SYSTEMS UNIT8: COMPUTERIZED NETWORK SYSTEMS

CFGS DAM
DPT INF

- ✓ Velocidad de transferencia medida en Mbps o Gbps
- ✓ Conectividad con el host: integrada, M.2, PCIe, USB, etc.
- ✓ Antenas: número de antenas y características.
- ✓ Seguridad: protocolos de seguridad como WEP, WPA, WPA2, WPA3, etc.

Existen adaptadores que integran otros tipos de adaptadores, como Wi-Fi y Bluetooth, o Wi-Fi y Ethernet.

8. Ficheros de configuración de red

Ubuntu emplea la herramienta NetPlan para gestionar y administrar la configuración de red. Desde Ubuntu 17.10, se emplea NetPlan con la intención de sustituir la configuración clásica anterior (a través del archivo `/etc/network/interfaces`)

Antes de realizar la configuración de la red, podemos conocer las interfaces de red identificadas por el sistema (para su posterior configuración) mediante los comandos.

`ip a`

`sudo lshw -class network`

El directorio `/etc/netplan/` alberga los archivos de configuración de NetPlan. Para las distribuciones Ubuntu Desktop, encontramos en dicho directorio los archivos: `01-network-manager-all.yaml` que establece la primera configuración, `02-network-manager-all.yaml` para la segunda (si se dispone), etc. De tal manera que se aplican estas configuraciones en el mismo orden numérico que el comienzo de su nombre. La configuración de estos archivos ha de realizarse con privilegios de administrador y debemos seguir la siguiente sintaxis, respetando los caracteres espacio:

```
Network:
  Version: 2
  Renderer: NetworkManager/networkd
  ethernet:
    Nombre_dispositivo:
      dhcp4: yes/no
      addresses: [DIRECCION_IP/MÁSCARA_DE_RED]
      gateway4: GATEWAY
      nameservers:
        addresses: [NOMBRE_1, NOMBRE_2]
```

COMPUTER SYSTEMS UNIT8: COMPUTERIZED NETWORK SYSTEMS

CFGS DAM
DPT INF

Donde:

- **Renderer:** nombre del gestor de red. NetworkManager es usado en sistemas de escritorio y networkd en servidores
- **Nombre dispositivo:** se sustituye por el nombre de la interfaz para configurar
- **dhcp4:** se indican los valores yes o no, si se configura por DHCP o con direccionamiento estático, respectivamente
- **addresses:** se indica la dirección IP con notación prefijo.
- **gateway4:** señala la puerta de enlace
- **nameservers:** indica las direcciones IP de los servidores DNS, siguiendo el formato indicado.

Ejemplo:

Veamos ejemplos de configuraciones:

- Configuración estática de una interfaz ethernet
- Configuración dinámica de una interfaz ethernet.

```
# Let NetworkManager manage all devices on this system
network:
  version: 2
  renderer: NetworkManager
  ethernet:
    enp0s3:
      dhcp4: no
      addresses: [192.168.1.8/24]
      gateway4: 192.168.1.1
      nameservers:
        addresses: [8.8.8.8, 8.8.8.4]
```

Ejemplo de configuración estática.

```
# Let NetworkManager manage all devices on this system
network:
  version: 2
  renderer: NetworkManager
  ethernet:
    enp0s3:
      dhcp4: yes
```

Ejemplo de configuración dinámica.

Para establecer los cambios, utilizamos el comando **netplan apply**. Y, por último, comprobamos los cambios en las interfaces con **ip address show**. Veamos el proceso completo en la imagen siguiente.

COMPUTER SYSTEMS UNIT8: COMPUTERIZED NETWORK SYSTEMS

CFGS DAM
DPT INF

```
gema@ubuntuvm:~$ cat /etc/netplan/01-network-manager-all.yaml
# Let NetworkManager manage all devices on this system
network:
  version: 2
  renderer: NetworkManager
  ethernets:
    enp0s3:
      dhcp4: yes

gema@ubuntuvm:~$ sudo netplan apply
[sudo] contraseña para gema:
gema@ubuntuvm:~$ ip address show enp0s3
2: enp0s3: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc fq_codel state UP group default qlen 1000
    link/ether 08:00:27:2e:b7:54 brd ff:ff:ff:ff:ff:ff
    inet 192.168.0.106/24 brd 192.168.0.255 scope global dynamic noprefixroute enp0s3
        valid_lft 7191sec preferred_lft 7191sec
    inet6 fe80::a00:27ff:fe2e:b754/64 scope link
        valid_lft forever preferred_lft forever
```

El orden de los mecanismos de resolución de nombres en los sistemas GNU/Linux viene establecido en el fichero `/etc/nsswitch.conf`. Este archivo es editable por el administrador del sistema, pudiendo modificar los mecanismos o su orden de aplicación.

```
hosts:          files mdns4_minimal [NOTFOUND=return] dns
```

Línea del fichero `/etc/nsswitch.conf` donde se especifica la resolución de nombres

Donde:

- ✓ files: fichero `/etc/hosts`
- ✓ mdns4_minimal [NOTFOUND=return]: utilizar el protocolo mDNS (para los nombres acabados en `.local`)
- ✓ dns: fichero `/etc/resolv.conf`

El archivo `/etc/hosts` contiene entradas con asignaciones entre direcciones IP y nombres de hosts. Por defecto y según la definición del fichero `/etc/nsswitch.conf`, el archivo `/etc/hosts` tiene prioridad sobre la configuración DNS del equipo, por lo que si se intenta resolver una dirección IP de un host coincidente con una entrada del archivo `/etc/hosts`, no se resolverá a través de DNS.

En Windows el archivo de configuración `hosts`: se encuentra en `c:\windows\system32\drivers\etc\` y se encarga de mantener un listado de asociaciones entre direcciones IP y dominios. Para agilizar la traducción de resolución de nombres de dominio, el orden en Microsoft Windows es el siguiente:

- Memoria caché del navegador web
- Archivo `hosts`

COMPUTER SYSTEMS UNIT8: COMPUTERIZED NETWORK SYSTEMS	CFGS DAM DPT INF
-----------------------------------------------------------------------	-----------------------------------

- Servidores DNS

Gracias a ello, al resolver localhost en un navegador web, se accede a la dirección IP 127.0.0.1 (definida esta asociación en el archivo hosts). Para editar este archivo, se debe realizar con privilegios de administrador, donde, por defecto, únicamente se define la interfaz de loopback (interfaz virtual de pruebas)

9. Monitorización y verificación de una red mediante comandos

Hemos visto cómo establecer la configuración de los adaptadores de red de manera permanente. No obstante, se pueden realizar modificaciones de las interfaces temporalmente empleando otros comandos.

Existen multitud de comandos que ayudan a monitorizar y verificar el correcto uso de la red.

Los principales comandos que permite monitorizar, mostrar información y configurar el entorno de red de un host en GNU/Linux son **ip** y **ss**.

El comando **ip** es muy potente. Las acciones de configuración de red más usuales son:

- ✓ Listar las interfaces activas e inactivas: **ip a**
- ✓ Deshabilitar una interfaz: **ip link set <interfaz> down**
- ✓ Habilitar una interfaz: **ip link set <interfaz> up**
- ✓ Configurar una interfaz: **ip addr add <dir_IP/mascara> dev <interfaz>**
- ✓ Eliminar una dirección IP: **ip addr del <dir_IP/mascara> dev <interfaz>**
- ✓ Mostrar la tabla de enrutamiento: **ip route show**
- ✓ Borrar una puerta de enlace predeterminada: **ip route del 0.0.0.0/0 via dir_IP dev <interfaz>**
- ✓ Añadir una puerta de enlace predeterminada: **ip route add 0.0.0.0/0 via dir_IP dev <interfaz>**
- ✓ Mostrar la tabla ARP: **ip neighbour show**

Nota: Es muy recomendable la lectura del comando **ip** (**man ip**) para mayor detalle.

COMPUTER SYSTEMS UNIT8: COMPUTERIZED NETWORK SYSTEMS

CFGs DAM
DPT INF

```
gema@ubuntuv:~$ sudo ip addr add 10.0.2.15/24 dev enp0s3
[sudo] contraseña para gema:
gema@ubuntuv:~$ ip a
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group default qlen 1000
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
    inet 127.0.0.1/8 scope host lo
        valid_lft forever preferred_lft forever
    inet6 ::1/128 scope host
        valid_lft forever preferred_lft forever
2: enp0s3: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc fq_codel state UP group default qlen 1000
    link/ether 08:00:27:2e:b7:54 brd ff:ff:ff:ff:ff:ff
    inet 192.168.0.109/24 brd 192.168.0.255 scope global dynamic noprefixroute enp0s3
        valid_lft 1570sec preferred_lft 1570sec
    inet 10.0.2.15/24 scope global enp0s3
        valid_lft forever preferred_lft forever
    inet6 fe80::a00:27ff:fe2e:b754/64 scope link
        valid_lft forever preferred_lft forever
gema@ubuntuv:~$
```

Otro comando muy utilizado y que también nos puede ayudar a identificar y mostrar multitud de detalles de las interfaces es **lshw**.

Para mostrar las asociaciones entre las direcciones físicas (MAC) y direcciones IP del segmento de red local en un equipo, se utilizan los comandos **arp** (en Microsoft Windows) e **ip neighbor show** (en GNU/Linux). Estas asociaciones se almacenan en una tabla ARP (también llamada caché ARP) y son necesarias para incluir las direcciones MAC en las tramas de la capa de enlace de datos. Su sintaxis es: **arp [opciones]**

Además, permite modificar las entradas de la tabla, dependiendo de las opciones aplicadas al comando.

Con ello, podemos detectar a qué equipos de su red se ha conectado un host gracias a las direcciones físicas de su tabla ARP.

COMPUTER SYSTEMS UNIT8: COMPUTERIZED NETWORK SYSTEMS

CFGS DAM
DPT INF

```
C:\windows\system32>arp -a
```

```
Interfaz: 192.168.0.104 --- 0x2
```

Dirección de Internet	Dirección física	Tipo
192.168.0.1	74-da-88-d2-12-98	dinámico
192.168.0.120	18-c0-4d-ab-61-e1	dinámico
224.0.0.2	01-00-5e-00-00-02	estático
224.0.0.22	01-00-5e-00-00-16	estático
224.0.0.251	01-00-5e-00-00-fb	estático
224.0.0.252	01-00-5e-00-00-fc	estático
239.255.255.250	01-00-5e-7f-ff-fa	estático
239.255.255.253	01-00-5e-7f-ff-fd	estático
255.255.255.255	ff-ff-ff-ff-ff-ff	estático

Ejecución comando arp -a

Los comandos con los que tradicionalmente se han monitorizado las interfaces de red han sido *ipconfig* (en Windows) e *ifconfig* (sustituido por *ip* y *ss* en Linux). Recomendamos emplear la ayuda de Microsoft Windows mediante *ipconfig -h*.

Otro de los comandos más empleados para comprobar una conexión de red es mediante el comando *ping*. Usado tanto en Windows como en Linux, este comando envía paquetes de prueba a un destino especificado y nos informa del tiempo de respuesta, en caso de existir conexión. Su sintaxis es la siguiente:

ping [opciones] destino

Donde *destino* es un nombre de dominio o la dirección IP. Para detener la salida por pantalla de los tiempos de respuesta, se utiliza la combinación de teclas Ctrl + C.

Gracias a él, podemos comprobar si un adaptador de red funciona correctamente o si se tiene acceso a otros equipos dentro de la red local o fuera de ella (Internet, por ejemplo). Con esto, podemos descartar multitud de errores y localizar un posible problema.

```
gema@ubuntuvn:~$ ping songandia.com
PING songandia.com (188.114.97.5) 56(84) bytes of data.
64 bytes from 188.114.97.5 (188.114.97.5): icmp_seq=1 ttl=54 time=13.1 ms
64 bytes from 188.114.97.5 (188.114.97.5): icmp_seq=2 ttl=54 time=14.1 ms
64 bytes from 188.114.97.5 (188.114.97.5): icmp_seq=3 ttl=54 time=15.1 ms
64 bytes from 188.114.97.5 (188.114.97.5): icmp_seq=4 ttl=54 time=13.7 ms
64 bytes from 188.114.97.5 (188.114.97.5): icmp_seq=5 ttl=54 time=14.1 ms
64 bytes from 188.114.97.5 (188.114.97.5): icmp_seq=6 ttl=54 time=17.8 ms
^C
--- songandia.com ping statistics ---
6 packets transmitted, 6 received, 0% packet loss, time 5008ms
rtt min/avg/max/mdev = 13.099/14.661/17.836/1.539 ms
```

COMPUTER SYSTEMS
UNIT8: COMPUTERIZED NETWORK SYSTEMS

CFGS DAM
DPT INF

Existen otras muchas aplicaciones que permiten realizar tareas de comprobación, monitorización, escaneo, verificación, auditoría, etc, entre las que destacamos Wireshark, Pandora FMS y Tcpdump.

Un complemento al comando ping para diagnosticar fallos de interconexión de redes es el comando **tracert** o **tracert**, en Ubuntu y Microsoft Windows respectivamente. Este permite conocer la ruta que sigue un paquete en la red (desde un origen IP a un destino IP), comprobando el estado de esta, los routers por los que pasa y localizar un posible fallo de conectividad. Su sintaxis es la siguiente:

- En Windows: **tracert** servidor_destino
- En Ubuntu: **tracert** servidor_destino

Otra herramienta ampliamente utilizada para realizar auditorías y funciones de seguridad de redes es **nmap**. Es un programa de código libre. En Linux se puede instalar a través de la línea de comandos y en Microsoft Windows, descargando e instalándolo desde nmap.org. Es una utilidad potente que permite escanear la red para inventariarla y monitorizarla.

nmap [opciones] objetivos

-----ACTIVIDAD 12-----

9.1. Gestión de puertos

En los sistemas informáticos en red, el término puerto puede hacer mención a:

- a) Puerto físico: entrada o conector de un dispositivo de red al que se conecta un medio de comunicación. Como, por ejemplo, un puerto RJ-45.
- b) Puerto lógico: número que se asocia a la aplicación de origen o destino de una comunicación. Son empleados por la capa de transportes, donde los segmentos especifican:
 - Puerto de origen: número que identifica la aplicación que origina la comunicación en el host.
 - Puerto de destino: número asociado a la aplicación de destino en el host remoto.

Por tanto, en las comunicaciones TCP y UDP los hosts han de indicar en el encabezado de cada segmento de la capa de transporte el número de puerto de origen y el número de puerto de destino.

Existen 3 tipos de puertos lógicos asociados a su número:

1. Puertos bien conocidos: número de 0 al 1023. Reservados para aplicaciones y servicios como HTTP(80), FTP(20), HTTPS(443), SMTP(25), etc.

COMPUTER SYSTEMS
UNIT8: COMPUTERIZED NETWORK SYSTEMS

CFGS DAM
DPT INF

2. Puertos registrados: números del 1024 al 49151. Son puertos empleados por las aplicaciones de usuario cuando conectan con servidores. En este rango se incluyen números de puertos registrados por la IANA para determinadas aplicaciones.
3. Puertos dinámicos, privados o efímeros: números 49152 al 65535. Son utilizados principalmente por aplicaciones de intercambio de archivos punto a punto.

De esta manera, si un usuario desea acceder a una página web, el proceso sería el siguiente. El host cliente indica en el encabezado del segmento de la capa de transporte el puerto de destino bien conocido 80 (ya que es un servicio HTTP) y, como puerto de origen, un número aleatorio a partir del 1024. De esta manera, se pueden establecer simultáneamente multitud de comunicaciones sobre un mismo servidor HTTP. Cuando el servidor se comunica con el cliente, este indica en el encabezado del segmento su puerto origen 80 y puerto destino el correspondiente a la aplicación y comunicación concreta del host cliente.

Como ya sabemos, los segmentos se encapsulan dentro de paquetes de la capa de red. Y en el encabezado de los paquetes de la capa de red se indican las direcciones IP de origen y destino. **A la combinación de una dirección IP y un puerto se le denomina socket.** Por tanto, una comunicación entre 2 hosts viene establecida por una pareja de sockets.

Un ejemplo de un socket es 192.168.1.55:80, formado por la dirección IP 192.168.1.55 y puerto 80. Este socket indica que pertenece a un servidor http, al ser un puerto bien conocido.

Los comandos que permiten monitorizar los puertos, sockets o conexiones de un sistema son *netstat*(Windows) y *ss*(GNU/Linux). Sus opciones son similares.

Son muchas las utilidades del comando *ss* que presenta la siguiente sintaxis:

ss [opciones] [filtro]

Algunas de las acciones más habituales para realizar con *ss* son:

- ✓ Mostrar información sobre las conexiones asociadas a los sockets **ss -a**
- ✓ Listar los sockets en escucha de nuestro host: **ss -l**
- ✓ Recoger estadísticas: **ss -s**

COMPUTER SYSTEMS
UNIT8: COMPUTERIZED NETWORK SYSTEMS

CFGS DAM
DPT INF

10. Resolución de problemas

La infraestructura de red y los sistemas informáticos en red requieren un mantenimiento que permita evitar averías o fallos y, si estos ocurren, actuar de manera planificada. El mantenimiento debe abordarse desde 3 ámbitos:

- Predictivo: se intenta pronosticar un futuro fallo para lo que se suelen emplear utilidades de diagnóstico.
- Preventivo: se lleva a cabo un Plan de mantenimiento preventivo, donde se detallan las acciones, técnicas y procedimientos a realizar, así como su frecuencia.
- Correctivo: se repara el objeto del fallo, siguiendo un Plan de mantenimiento correctivo que establece el método para diagnosticar y resolver averías.

Ya conocemos herramientas de diagnóstico donde podemos monitorizar y testear el estado y comunicación de los dispositivos de red: *ping*, *ifconfig* (*ipconfig* en Windows), *ss* (*netstat* en Windows), *lshw*, etc. Además de otras herramientas analizadas anteriormente, como los monitores de rendimiento y administradores de dispositivos que permiten estudiar el estado de los dispositivos de red y su rendimiento (con el Administrador de tareas de Windows o el Monitor del sistema GNOME en Linux).

También es recomendable apoyarse en aplicaciones especializadas para comprobar otros aspectos más concretos, según las necesidades de mantenimiento o resolución de averías. Ejemplo de ello es Wireshark, muy útil para analizar diferentes protocolos y filtrar el tráfico de la red en busca de vulnerabilidades. Así como muchas otras aplicaciones, que ayudan a planificar y resolver posibles problemas en entornos Wi-Fi, como, por ejemplo, WiFi Analyzer, WiFi HeatMap y NetSpot.

Los fallos o averías en el funcionamiento de los sistemas informáticos en red pueden ser muy variados. La experiencia y una planificación adecuada, mediante un Plan de mantenimiento correctivo adecuado, ante cualquier incidencia es fundamental para detectar y solventar el problema de la manera más eficiente posible.

Los principales fallos los podemos agrupar en:

COMPUTER SYSTEMS UNIT8: COMPUTERIZED NETWORK SYSTEMS

CFGS DAM
DPT INF

Fallos de los sistemas informáticos en red más comunes

Fallos		Comprobaciones
Fallos en hosts		
Fallos en la tarjeta de red	Tarjeta averiada	Probar otra tarjeta de red en el equipo.
	Tarjeta mal instalada	Comprobar la correcta instalación hardware y software, mediante drivers adecuados al sistema operativo.
Fallos en la configuración de la tarjeta de red	Configuración TCP/IP inadecuada	Revisar los valores: dirección IP, máscara de red, Gateway y DNS. En su caso, habilitar la opción DHCP.
	Configuración Wi-Fi inadecuada y baja señal	Comprobar el tipo de autenticación Wi-Fi y la contraseña. Testear la cobertura de la señal inalámbrica, debiendo ser adecuada la finalidad de la red, sin verse mermada por ruido electromagnético o una mala ubicación del punto de acceso o el dispositivo inalámbrico.
Fallos en el medio		
Fallos en cableado		Chequear que no se sobrepasa el radio de curvatura máximo y que no se encuentra forzado, aplastado o roto. Cerciorarse que el tipo de cableado es adecuado al ruido electromagnético del entorno. En cables de fibra óptica, la pérdida de señal ha de ser la mínima posible en el proceso de fusión.
Fallos en conectores		Revisar que los conectores y puertos no están forzados y sucios. Los cables han de estar bien engastados en su interior. Comprobar el mapa de cableado, según los estándares TIA/EIA para cobre de par trenzado.
Fallos en la electrónica de red		
Configuración inadecuada de puntos de acceso Wi-Fi		Revisar la configuración de la autenticación Wi-Fi, filtros MAC, SSID oculto, DHCP, conjunto de direcciones estáticas, etc. Debe estar correctamente conectado con el sistema de distribución.
Problemas en switches		Chequear que el switch está encendido, con conectividad por los indicadores de estado led de cada puerto y a una temperatura de trabajo óptima.

Nota: Las herramientas hardware más utilizadas para comprobar los diferentes medios de transmisión de datos son:

- ✓ Certificadora de fibra óptica y cobre. Herramienta muy completa que permite medir la pérdida de potencia de la fibra, detectar distancias exactas o cortes de fibra óptica, comprobación y certificación de redes de cobre y fibra óptica y estudiar otros muchos parámetros.
- ✓ Inspector de fibra óptica. Muestra el estado de conectores de fibra óptica.

COMPUTER SYSTEMS UNIT8: COMPUTERIZED NETWORK SYSTEMS

CFGS DAM
DPT INF

- ✓ Analizador de cableado de cobre de par trenzado. Consta de dos módulos, uno transmite un pulso eléctrico por un extremo y el otro módulo permite seguirlo, sin necesidad de desconectar cables, al pasar por encima de estos y emitir un sonido.
- ✓ Analizador de redes inalámbricas. Realiza un estudio del estado de la señal inalámbrica: pruebas de conexión, vulnerabilidades, cobertura, etc



Inspector de fibra óptica

11. Seguridad en las comunicaciones

La seguridad de los sistemas informáticos está íntimamente asociada a la seguridad en las comunicaciones, ya que hoy en día uno está integrado en el otro.

Para que las comunicaciones entre sistemas sean seguras, estas han de basarse en 4 pilares fundamentales:

1. Los accesos a la información, a los sistemas y a los recursos han de ser confidenciales, es decir, solo se permite el acceso a aquellos usuarios o procesos autorizados.
2. La información o los recursos han de estar disponibles para los usuarios o procesos con permisos.
3. La modificación de la información o recursos debe realizarse por procesos o usuarios autorizados, de esta manera, se garantiza la integridad de los mismos.
4. Se debe garantizar la autenticidad. Para ello, se tiene que confirmar la identidad del emisor y del receptor:
 - El emisor debe asegurar al receptor que los datos han sido enviados por él
 - El receptor debe asegurar al emisor que los datos han sido recibidos por él.

COMPUTER SYSTEMS UNIT8: COMPUTERIZED NETWORK SYSTEMS	CFGS DAM DPT INF
-----------------------------------------------------------------------	-----------------------------------

Para lograrlo, primero se deben establecer unas políticas de seguridad a partir de planes de contingencia y seguridad.

11.1. Políticas de seguridad

En cualquier sistema informático, se necesita establecer políticas o planes de seguridad basados en los elementos que se van a proteger. Para ello, periódicamente se debe realizar un análisis de riesgos, donde se evalúen los recursos, la infraestructura de red y los sistemas, estableciendo sus puntos débiles. Basándose en los anteriores, se definirán planes de contingencia y seguridad centrados en los pilares de la seguridad en las comunicaciones: confidencialidad, disponibilidad, integridad y autenticidad.

En entornos empresariales e instituciones públicas o privadas, se deben difundir las políticas de seguridad y aquellas normas o procedimientos necesarios para que todos los usuarios conozcan los criterios y métodos para abordar la seguridad. Las más destacables son:

- ✓ Políticas de contraseñas
- ✓ Política de actualizaciones
- ✓ Política de uso de correo electrónico
- ✓ Políticas de aplicaciones permitidas
- ✓ Políticas de uso de conexiones externas
- ✓ Políticas de almacenamiento y copias de seguridad
- ✓ Políticas de uso de portátiles corporativos
- ✓ Políticas de dispositivos personales.

En ellas se detallan aspectos de seguridad, como:

- Empleo de contraseñas robustas y actualización periódica de las mismas
- Uso de aplicaciones conocidas y actualizadas.
- Actualización y mantenimiento de cuentas de usuarios
- No difusión de cuentas y contraseñas a terceros
- No ejecución de aplicaciones desconocidas o sin verificar procedentes del exterior: email, medios de almacenamiento externos, red externa, etc.
- Actualización y mantenimiento activo del sistema operativo y las aplicaciones
- Creación y mantenimiento de las copias de seguridad
- Monitorización de la red
- Protección antimalware
- Control de acceso físico a los sistemas y medios de red

COMPUTER SYSTEMS UNIT8: COMPUTERIZED NETWORK SYSTEMS	CFGS DAM DPT INF
-----------------------------------------------------------------------	-----------------------------------

- Configuración segura de las redes inalámbricas.

11.2. Tipos de ataques

Un ataque informático es una acción ofensiva y deliberada que intenta tomar información, dañar, alterar, desestabilizar o destruir datos, información o sistemas informáticos independientes o en red.

Se distinguen los ataques activos (aquellos que ocasionan cambios en la información o los recursos) de los pasivos (que simplemente monitorizan, registran o acceden a los recursos, sin alterar estos o su información). Los ataques más usuales son:

- a) Reconocimiento y detección de vulnerabilidades en los sistemas. Tratan de obtener información del sistema, sin provocar daño alguno, de vulnerabilidades para su posterior explotación.
- b) Interceptación de información. Tratan de interceptar datos enviados en red, vulnerando la confidencialidad.
- c) Modificación de información. Reenvían mensajes o documentos alterados de manera premeditada que han sido previamente interceptados. De esta manera, se vulnera la integridad, autenticidad y confidencialidad.
- d) Suplantación de identidad. Son muchos los tipos de ataques de este tipo que afectan a la integridad, autenticidad y confidencialidad, como, por ejemplo:
 - Captura de cuentas de usuario y contraseñas
 - SMTP Spoofing: envío de emails con remitentes falsos suplantando su identidad
 - IO Spoofing: envío de paquetes IP desde un host distinto al que realmente lo ha enviado.
 - DNS Spoofing: direccionamiento erróneo de nombres de dominio.

11.3. Mecanismos de seguridad en las comunicaciones

Con objeto de proteger las comunicaciones, se pueden emplear un conjunto de herramientas variadas. Su uso o aplicación dependerá de las necesidades establecidas en los planes de contingencia y seguridad. Para lograrlo, podemos utilizar un canal seguro de comunicaciones, o que el mensaje en sí sea seguro. Por tanto, las herramientas más empleadas son:

- ✓ Filtros de contenido. Software que se encarga de gestionar, restringir y limitar el acceso a sitios web con el propósito de evitar contenidos maliciosos o de dudosa intención.
- ✓ Redes privadas virtuales o VPN. Consisten en la creación de una extensión de una red local a través de una red pública (como Internet), de tal manera que se pueda establecer una conexión virtual segura punto a punto. Se pueden realizar desde los propios sistemas operativos o mediante aplicaciones específicas. Son muy amplios sus usos:

COMPUTER SYSTEMS
UNIT8: COMPUTERIZED NETWORK SYSTEMS

CFGS DAM
DPT INF

- Navegar de manera anònima
- Descarga P2P
- Obtener un extra de seguridad en las comunicaciones
- Teletrabajo
- ✓ Cortafuegos o firewall. Son herramientas (hardware o software) que controlan el tráfico entrante y saliente. Limitan o bloquean el tráfico externo, normalmente de Internet, para evitar accesos no autorizados a otra red (generalmente privada)
- ✓ Software antimalware
- ✓ Herramientas de cifrado. Permiten cifrar datos a través de redes inseguras de tal manera que se garantice la confidencialidad, autenticidad e integridad. Consisten en aplicar un algoritmo que transforme un mensaje a partir de una clave. Existen 2 tipos de cifrado:
 1. Cifrado simétrico: solo se emplea una clave para cifrar y descifrar. Aporta confidencialidad
 2. Cifrado asimétrico: se emplean 2 claves, una privada y otra pública. A partir de la clave pública no se puede averiguar la clave privada. Aporta autenticidad, integridad y no repudio (no se puede negar la recepción o envío de un mensaje). La clave pública cifra el mensaje y la clave privada lo descifra. Únicamente el emisor posee su clave privada y hace llegar su clave pública a aquellos que quieran comunicarse (cifrando el mensaje) con él.
- ✓ Emplea de protocolos seguros, como SSL/TLS, Open SSL o GnuTLS, HTTPS, SFTP, etc.