UD8 SISTEMAS INFORMÁTICOS EN RED. CONFIGURACIÓN Y EXPLOTACIÓN

1. Protocolos principales de red

Los sistemas informáticos actuales se consideran sistemas en red, donde los dispositivos están conectados para compartir información. Estos sistemas se basan en modelos de referencia que establecen las características y especificaciones necesarias para la comunicación entre entidades y el intercambio de información. Los modelos de referencia más utilizados son el modelo OSI y el modelo TCP/IP.

El modelo OSI (Open Systems Interconnection) se divide en siete niveles o capas, cada una con funciones específicas. Estas capas se comunican entre sí, y el proceso de comunicación entre un emisor y un receptor sigue un recorrido a través de estas capas. Cada capa agrega metainformación a los datos de la capa superior, en un proceso llamado encapsulamiento. Las capas del modelo OSI y sus funciones son:

- **Aplicación:** Interfaz entre el usuario y las aplicaciones.
- **Presentación:** Determina el formato de la información y puede comprimirla o cifrarla.
- **Sesión:** Establece, mantiene y controla el diálogo entre aplicaciones.
- **Transporte:** Prepara y controla el flujo de datos entre emisor y receptor.
- **Red:** Selecciona la ruta entre emisor y receptor.
- **Enlace de datos:** Detecta y corrige errores en la transmisión de datos.
- **Física:** Establece las especificaciones del enlace físico de transmisión.

Las cuatro capas inferiores se encargan del transporte y el control del flujo de datos, mientras que las tres capas superiores están relacionadas con las aplicaciones.

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	

Por otro lado, el modelo TCP/IP es el estándar abierto de Internet y se adapta al modelo OSI. El nombre del modelo TCP/IP proviene de los protocolos TCP (Transmission Control Protocol) e IP (Internet Protocol). Cada capa del modelo TCP/IP tiene múltiples protocolos asociados. Algunos protocolos conocidos son TCP, IP, HTTP, FTP y DNS.

Protocolos destacados del modelo TCP/IP

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

En resumen, los protocolos de red se basan en modelos de referencia como el modelo OSI y el modelo TCP/IP. Estos modelos descomponen las funciones de comunicación en varias capas para definir protocolos y estándares, controlar el flujo de datos y facilitar la evolución de las redes de comunicación.

1.1. Protocolo Ethernet (capa OSI física)

El protocolo Ethernet es utilizado en redes de área local (LAN) y establece la conexión y transmisión de datos a través de cables. Utiliza el mecanismo CSMA/CD para gestionar el acceso al medio compartido, evitando colisiones entre las transmisiones de diferentes hosts. Ethernet es ampliamente utilizado debido a su bajo costo, flexibilidad, facilidad de implementación y seguridad.

1.2. Protocolo Wi-Fi (capa OSI física)

Por otro lado, el protocolo Wi-Fi se utiliza en redes de área local inalámbricas y define especificaciones para la transmisión de datos por radiofrecuencia. Emplea el mecanismo CSMA/CA, que reduce las colisiones en el medio inalámbrico. La principal ventaja de Wi-Fi es su facilidad de instalación y movilidad, pero tiene desventajas en cuanto a seguridad y saturación de canales, lo que puede aumentar la latencia en las comunicaciones.

Ambos protocolos tienen estándares que se mejoran con el tiempo para adaptarse a las necesidades tecnológicas.

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 (Internet Protocol) es utilizado en el modelo TCP/IP y se encarga del enrutamiento de paquetes de datos. Decide la ruta óptima para transportar los paquetes desde el origen hasta el destino, pasando por nodos intermedios. Además, utiliza direcciones IP para identificar de manera única cada dispositivo de red.

El protocolo IP no garantiza la entrega confiable de paquetes ni el orden en que llegan. Sin embargo, otros protocolos de capas superiores, como TCP (Transmission Control Protocol), pueden proporcionar esta funcionalidad.

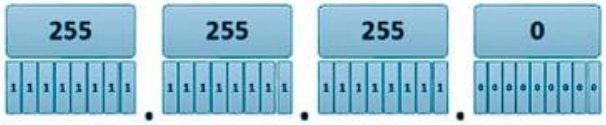
Las direcciones IP se asignan a las interfaces de red de los dispositivos y son necesarias para enviar y recibir paquetes. Es importante que no haya duplicación de direcciones IP en una misma red, ya que esto causaría conflictos y errores en la comunicación.

En la actualidad, se utilizan dos versiones principales del protocolo IP: IPv4 e IPv6. IPv4 es la versión más antigua y utiliza direcciones de 32 bits, lo que limita la cantidad de direcciones disponibles. Por otro lado, IPv6 es la versión más reciente y utiliza direcciones de 128 bits, lo que permite un número mucho mayor de direcciones disponibles para satisfacer las necesidades de la creciente cantidad de dispositivos conectados a Internet.

1.3.1. Protocolo IPv4

El protocolo IPv4 es utilizado para asignar direcciones IP en redes. Utiliza un formato de 32 bits dividido en 4 bloques de 8 bits, donde cada bloque representa un número entre 0 y 255. Se utiliza una máscara de red para identificar la porción de red y la porción de host en una dirección IP. La máscara de red puede expresarse como una dirección IP con el número de unos que contiene, utilizando la notación CIDR.

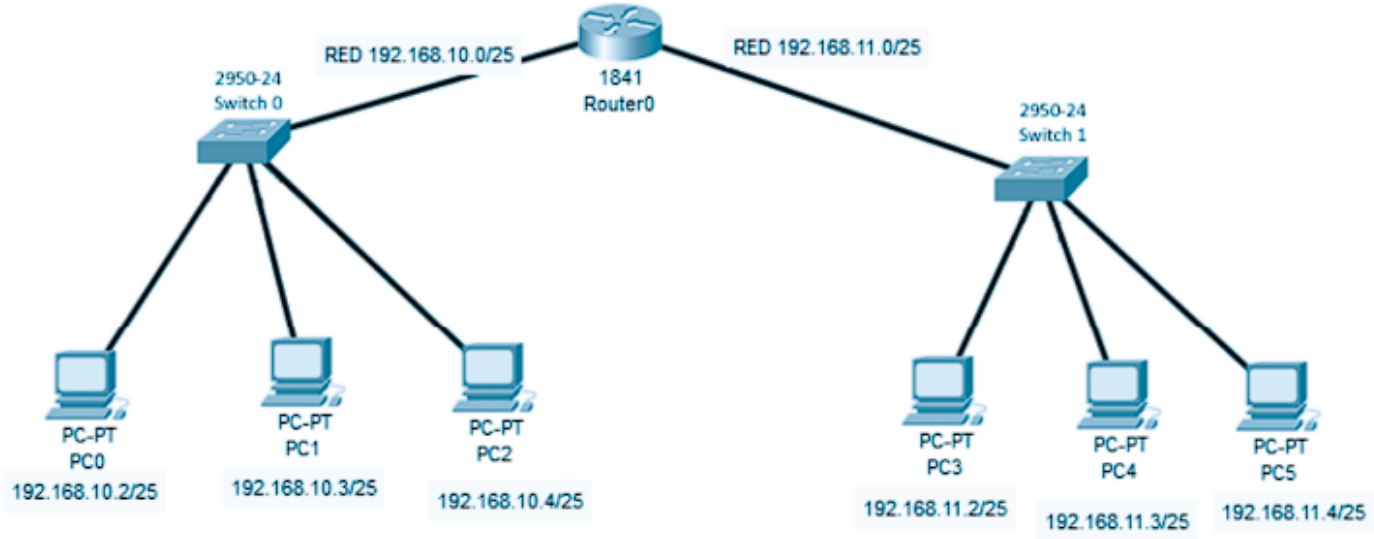
Ejemplo de dirección IP.



Ejemplo de máscara de red.

Dentro del rango de direcciones IP de una red, se encuentran diferentes tipos de direcciones. La dirección de red representa la red y tiene todos los bits de la porción de host en 0. La dirección de broadcast se utiliza para enviar paquetes a todos los hosts de la red y tiene todos los bits de la porción de host en 1. Las direcciones de hosts son asignadas a dispositivos dentro de la red.

En el diseño lógico de una red, se pueden utilizar direcciones IP públicas o privadas. Las direcciones IP públicas son únicas a nivel mundial y se asignan para su uso en Internet. Las direcciones IP privadas están destinadas a redes con acceso restringido o nulo a Internet y se asignan dentro de bloques específicos. Los routers se encargan de traducir las direcciones IP privadas a públicas y viceversa mediante el protocolo NAT.



	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

	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

Además de la dirección IP, los adaptadores de red tienen una dirección física llamada dirección MAC, que es única a nivel mundial. Esta dirección, compuesta por 48 bits y representada en formato hexadecimal, es utilizada por la capa de enlace de datos del modelo OSI para identificar el origen y el destino de las tramas en el protocolo Ethernet.

1.3.2. Protocolo IPv6

El protocolo IPv6 es la versión actualizada del protocolo IP y utiliza direcciones de 128 bits. Estas direcciones se representan en hexadecimal en bloques de 2 bytes. IPv6 ofrece varias ventajas, como un aumento en la seguridad de la comunicación, un mejor tratamiento de los paquetes y un mayor número de direcciones IP disponibles, lo que permite implementar el Internet de Todo (IoE).

Para abreviar las direcciones IPv6, se aplican ciertas reglas. El bloque "0000" se reduce a "0". Si hay dos o más bloques consecutivos con valor 0, se pueden representar con "::" una sola vez en la dirección. Los ceros a la izquierda también se pueden descartar. Por ejemplo, la dirección "5560:0088:0000:0000:F103:31AA:75AC:0000" se puede abreviar como "5560:88::F103:31AA:75AC:0".

Además, una dirección IPv4 se puede representar en notación IPv6 como "0:0:192:168.1.5" o "::192.168.1.5".

1.4. Protocolo TCP y UDP (capa OSI transporte)

TCP y UDP son protocolos de transporte en la capa OSI. TCP es confiable pero más lento, garantizando la entrega de todos los segmentos. UDP es rápido pero no confiable, ya que puede perder algunos segmentos. TCP se usa en aplicaciones que necesitan confiabilidad (FTP, HTTP), mientras que UDP se usa en aplicaciones de streaming de video y audio.

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

En la configuración estática, se utiliza una dirección IP fija que no cambia con el tiempo y es adecuada para servidores de Internet y servicios como impresión, HTTP y FTP. Para configurar una dirección IP estática en Windows, se accede a las propiedades del adaptador de red a través del Centro de redes y recursos compartidos. Se deben proporcionar los datos de la dirección IP, máscara de subred, puerta de enlace predeterminada y servidores DNS. En Ubuntu, la configuración estática se realiza a través de la opción Red en Configuración, donde se ingresan los datos en la pestaña IPv4 seleccionando el modo Manual.

2.2. Dinámica

En la configuración dinámica del protocolo TCP/IP, la dirección IP se asigna de forma automática y cambia con el tiempo. Esto se logra mediante el protocolo DHCP, que utiliza un servidor DHCP para proporcionar la configuración necesaria a los clientes DHCP, como la dirección IP, máscara de red, servidor DNS y puerta de enlace. Los routers SoHo suelen tener un servidor DHCP habilitado de forma predeterminada. Los servidores DHCP permiten establecer el rango de direcciones asignables por este protocolo, reservando el resto de direcciones para el direccionamiento estático. En la configuración TCP/IP de los clientes DHCP, se transfieren los datos proporcionados por el servidor DHCP. Para obtener una dirección IP dinámica, se mantiene la configuración del Protocolo de Internet versión 4 (TCP/IPv4) en automático.

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.

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 única-mente.
	Punto de acceso	Extiende la red cableada mediante un medio inalámbrico. Pertenece 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 retransmitiré al puerto de destino y no a todos los restantes.

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

Los routers son dispositivos que conectan diferentes redes y existen dos tipos: rackeables o empresariales y routers SoHo. Tanto los routers como los hosts utilizan tablas de enrutamiento para enviar paquetes. Los hosts tienen tablas de enrutamiento simples, mientras que los routers tienen tablas más complejas. Las tablas de enrutamiento de los routers contienen conexiones locales, estáticas y dinámicas.

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

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:

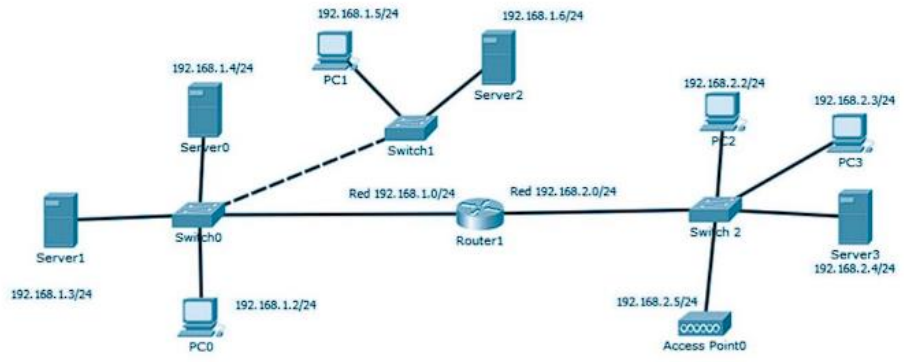
3.3.1. Topología física

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)
  - Redes de área local (LAN)

3.3.2. Topología lógica

Se establece la configuración de comunicación y acceso al medio para cada elemento de red. En redes WAN, hay conexiones punto a punto entre dos equipos. En redes LAN, se utilizan métodos de acceso por contienda y acceso controlado para controlar el acceso al medio compartido. En el mapa lógico, se muestra la conexión entre diferentes elementos de red, como equipos, direcciones IP y líneas de conexión. En el mapa físico, se representan las estancias, los dispositivos de red y los componentes en los racks.



Ejemplo de mapa lógico.

3.4. Dominios de colisión y difusión

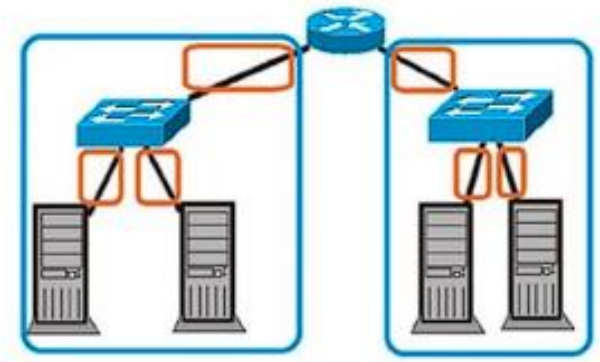
Los dispositivos de capa 2 o superiores, como los routers y switches, dividen los dominios de colisión (áreas donde pueden colisionar paquetes). Además, los dispositivos de capa 3 o superiores, como los routers, dividen los dominios de difusión (áreas donde se reciben tramas de broadcast).

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).

Dominios de colisión.



Dominios de colisión.

4. Tipos de redes

Las redes se clasifican de la siguiente manera:

A) Según su tamaño:

- Redes de área personal (PAN): entorno del usuario, como Bluetooth o NFC.
- Redes de área local (LAN): WLAN para redes inalámbricas.
- Redes de área metropolitana (MAN): intermedias entre LAN y WAN, conectando varias redes LAN.
- Redes de área extensa (WAN): de larga distancia que conectan redes LAN o WAN.

B) Según su transmisión:

- Redes punto a punto: transmisión de un origen a un destino a través de un medio.
- Redes multipunto: transmisión de un origen a múltiples destinos compartiendo el mismo medio.

C) Según su función:

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

D) Según los medios empleados:

- Redes inalámbricas: utilizan ondas electromagnéticas como Bluetooth y Wi-Fi.
- Redes cableadas: utilizan medios físicos como cables de cobre o fibra óptica.
- Redes 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 subscribirse 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:

- Conmutación de circuitos: se establece un circuito dedicado entre los nodos antes de la comunicación. Ejemplo: red telefónica conmutada.
- Conmutación de paquetes: los datos se dividen en paquetes y se transmiten a través de una red compartida. No es necesario establecer un circuito previamente. Es más económica pero tiene mayor latencia.
- Conexión dedicada: proporciona una conexión directa y permanente entre dos nodos de la red WAN del proveedor de servicios. Es costosa pero reduce la latencia, ideal para VoIP y video sobre IP.

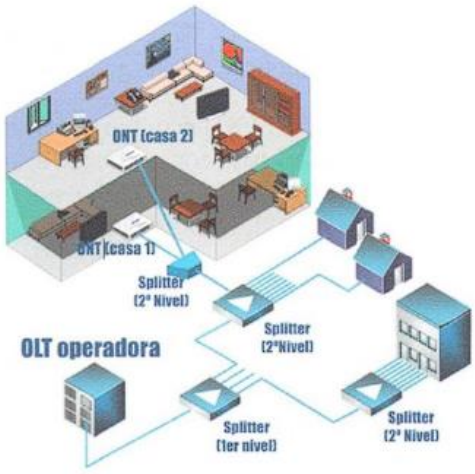


Figura 5.16
Elementos de conexión FTTH.
Fuente: http://fibraopticahastaelhogarecuador.

5.2. Conexiones WAN públicas

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

- 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.
- Fibra hasta el hogar: alcanza velocidades muy superiores a la familia DSL, empleando fibra óptica desde la red troncal hasta los clientes.
- 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, son muy empleadas en redes WAN:
    - WiMAX: Es ideal para zonas que no dispongan de cobertura por cable.
    - LTE-A (4G) y 5G: permiten gran movilidad de los terminales inalámbricos.

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:

6.1.1. 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.

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

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 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.

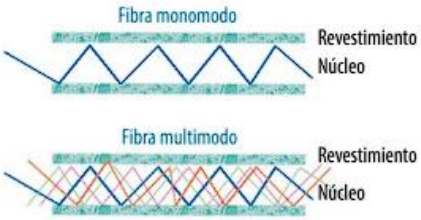
6.1.2. Cable de fibra óptica

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
- Según el modo de transmisión
    - Monomodo: se emite un único haz de luz por el interior del hilo. Es empleado principalmente para largas distancias.
    - Multimodo: transmite varios haces de luz con diferentes trayectorias. Se suele utilizar para distancias cortas (entre manzanas de edificios o en el interior de estos).

Estructura de cables de fibra óptica.



Transmisión en fibra óptica.

6.2. Dispositivos de interconexión

Los switches y routers son elementos clave en la infraestructura de red para conectar cables de par trenzado. Se instalan en armarios de distribución o racks que contienen otros elementos como paneles de parcheo, regletas eléctricas, bandejas y organizadores de cables. También existen dispositivos de interconexión y adaptadores de red para fibra óptica y cables mixtos de par trenzado y fibra óptica.

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:

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

7. Redes inalámbricas

Las redes inalámbricas aportan ventajas con respecto a las redes cableadas, como la movilidad, la flexibilidad y la facilidad de instalación.

7.1. Tipos y características

Las redes inalámbricas más comunes incluyen Wi-Fi, WiMAX, 4G y 5G, así como Bluetooth y Zigbee para redes WPAN.

Cada una tiene características distintas que las hacen más adecuadas para diferentes aplicaciones. Sin embargo, estas características pueden afectar la capacidad de transmisión debido a factores como el colapso de la banda de trabajo, interferencias electromagnéticas, número de usuarios conectados, ubicación de las antenas y el uso en interiores o exteriores.

7.1.1. 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.

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.

7.1.2. WiMAX

Establece una red de comunicación de alta velocidad para redes MAN.

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.

7.1.3. 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.

La generación 5G, pudiendo alcanzar 20 Gbps. Es ideal para aplicaciones en tiempo real y el desarrollo del IoT (Internet de las Cosas).

7.1.4. 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:

- 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 rea 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:

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

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 dispositivos que deseen conectarse a una red inalámbrica necesitan adaptadores de red inalámbricos específicos para el tipo de red al que desean conectarse. Estos adaptadores pueden estar integrados en el hardware de dispositivos como smartphones, portátiles y placas base de computadoras de escritorio, o se pueden adquirir como dispositivos externos o internos.

Algunas características importantes de los adaptadores de red Wi-Fi incluyen los estándares Wi-Fi compatibles, las bandas de frecuencia utilizadas, la velocidad de transferencia, el tipo de conectividad con el host, el número y características de las antenas, y los protocolos de seguridad soportados. También existen adaptadores que combinan diferentes tipos de conectividad, como Wi-Fi y Bluetooth, o Wi-Fi y Ethernet.

8. Ficheros de configuración de red

Ubuntu utiliza la herramienta NetPlan para administrar la configuración de red, reemplazando la configuración clásica a través del archivo "/etc/network/interfaces" desde Ubuntu 17.10. Se pueden utilizar comandos como "ip a" y "sudo lshw -class network" para conocer las interfaces de red identificadas por el sistema antes de configurar la red.

Los archivos de configuración de NetPlan se encuentran en el directorio "/etc/netplan/". Para distribuciones de Ubuntu Desktop, los archivos de configuración suelen tener nombres como "01-networkmanager-all.yaml" y "02-network-manager-all.yaml", y se aplican en orden numérico. La configuración se realiza con privilegios de administrador y sigue

una sintaxis específica, incluyendo el nombre del gestor de red, el nombre del dispositivo, la configuración DHCP o estática, direcciones IP, puerta de enlace y servidores DNS.

Se pueden encontrar ejemplos de configuraciones estáticas y dinámicas de interfaces Ethernet. Los cambios se aplican utilizando el comando "netplan apply" y se pueden verificar utilizando "ip address show".

En GNU/Linux, el orden de los mecanismos de resolución de nombres se especifica en el archivo "/etc/nsswitch.conf", y se puede modificar según las necesidades del administrador del sistema. El archivo "/etc/hosts" contiene asignaciones de direcciones IP a nombres de hosts y tiene prioridad sobre la configuración DNS del equipo. En Windows, el archivo de configuración equivalente se encuentra en "c:\windows\system32\drivers\etc" y sigue un orden de resolución que incluye la memoria caché del navegador, el archivo hosts y los servidores DNS.

9. Monitorización y verificación de una red mediante comandos

La herramienta NetPlan se utiliza en Ubuntu para administrar la configuración de red, reemplazando la configuración anterior a través del archivo "/etc/network/interfaces". Se pueden utilizar comandos como "ip a" y "sudo lshw -class network" para identificar las interfaces de red en el sistema.

Los archivos de configuración de NetPlan se encuentran en el directorio "/etc/netplan/". Se deben seguir cierta sintaxis al configurar los archivos, incluyendo el nombre del gestor de red, el nombre de la interfaz, el tipo de configuración (DHCP o estática), direcciones IP, puerta de enlace, servidores DNS, etc.

En GNU/Linux, el archivo "/etc/nsswitch.conf" determina el orden de los mecanismos de resolución de nombres. El archivo "/etc/hosts" contiene asociaciones entre direcciones IP y nombres de hosts, y tiene prioridad sobre la configuración DNS.

En Windows, el archivo de configuración hosts se encuentra en "c:\windows\system32\drivers\etc" y se utiliza para asociaciones entre direcciones IP y dominios. El orden de resolución de nombres en Windows incluye la memoria caché del navegador web, el archivo hosts y los servidores DNS.

9.1. Gestión de puertos

En los sistemas informáticos en red, el término "puerto" puede referirse a un puerto físico (conector de un dispositivo de red) o a un puerto lógico (número asociado a una aplicación de origen o destino en una comunicación). Los puertos lógicos se utilizan en las comunicaciones TCP y UDP para identificar las aplicaciones.

Existen tres tipos de puertos lógicos: puertos bien conocidos (del 0 al 1023) reservados para servicios como HTTP, FTP, etc.; puertos registrados (del 1024 al 49151) utilizados por aplicaciones de usuario; y puertos dinámicos, privados o efímeros (del 49152 al 65535) usados principalmente por aplicaciones de intercambio de archivos punto a punto.

Los puertos lógicos junto con las direcciones IP forman los sockets, que representan una comunicación entre dos hosts. Por ejemplo, el socket 192.168.1.55:80 indica la dirección IP 192.168.1.55 y el puerto 80, correspondiente a un servidor HTTP.

Los comandos "netstat" en Windows y "ss" en GNU/Linux permiten monitorizar los puertos, sockets y conexiones de un sistema, ofreciendo información y estadísticas sobre ellos.

10. Resolución de problemas

El mantenimiento de la infraestructura de red y los sistemas informáticos en red se divide en tres ámbitos: predictivo, preventivo y correctivo. El mantenimiento predictivo consiste en pronosticar posibles fallos mediante herramientas de diagnóstico. El mantenimiento preventivo implica seguir un plan detallado de acciones y procedimientos para evitar averías. El mantenimiento correctivo repara los fallos siguiendo un plan que establece cómo diagnosticar y resolver las averías.

Existen herramientas de diagnóstico como ping, ifconfig (ipconfig en Windows), ss (netstat en Windows) y lshw para monitorizar y probar el estado y la comunicación de los dispositivos de red. También se recomienda utilizar aplicaciones

especializadas como Wireshark para analizar protocolos y buscar vulnerabilidades en el tráfico de red, así como otras herramientas específicas para resolver problemas en entornos Wi-Fi.

Los fallos en los sistemas informáticos en red pueden ser diversos, por lo que es importante contar con experiencia y una planificación adecuada para detectar y solucionar los problemas de manera eficiente.

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.

Además, se mencionan algunas herramientas hardware utilizadas para comprobar los medios de transmisión de datos, como certificadoras de fibra óptica y cobre, inspectores de fibra óptica, analizadores de cableado de cobre de par trenzado y analizadores de redes inalámbricas.

En resumen, el mantenimiento de los sistemas informáticos en red se realiza de forma predictiva, preventiva y correctiva, utilizando herramientas de diagnóstico y aplicaciones especializadas, y considerando diferentes fallos que pueden ocurrir.