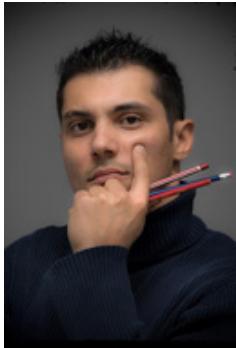


Caracterización de Redes.

Caso práctico

En la segunda quincena de marzo la empresa **BK Sistemas Informáticos** se encuentra cada curso con la llegada de alumnado de Formación Profesional (FP) para realizar el módulo de Formación en Centros de Trabajo (FCT).

Es una empresa que ofrece diversos servicios informáticos a otras empresas con **Juan** como responsable del departamento de Informática y que ha encontrado en esta colaboración con los Institutos de FP la mejor forma de encontrar personal cualificado, participando en la formación del alumnado que viene integrando en su plantilla durante los últimos años, como ha pasado con **Laro**, reciente titulado en ASIR.



[Alain Bachellier \(CC BY-NC-SA\)](#)

Durante el periodo que **Laro** realizó de FCT en BK Sistemas Informáticos conoció a **Vindio**, empleado de la empresa que le ayudó en todo, con quien ha entablado amistad, y a quien le está muy agradecido, no solo por la implicación demostrada en su formación y por la ayuda prestada en todo momento, sino también por su capacidad de trabajo y dominio de todos los servicios que presta la empresa. Es su referente y por quien siente admiración.

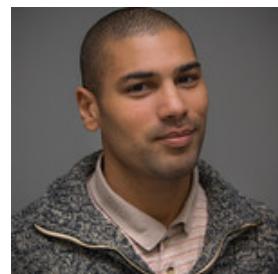
Como cada lunes a las 8:00h, se ha realizado la reunión del departamento de Informática y Juan ha informado de dos temas importantes que afectan principalmente a **Laro** y **Vindio**:

- 1.- La instalación de una red local en la renovación del Aula de Formación de la propia empresa.
- 2.- La incorporación de tres alumnas del ciclo de ASIR para realizar la FCT y que deben tutorizar entre ambos.

La primera pregunta que se hace Laro ante esta información es... ¿Qué tipo de red tenemos que instalar?



[Jonny Goldstein \(CC BY\)](#)



[Alain Bachellier \(CC BY-NC-SA\)](#)

En esta unidad de trabajo se va a estudiar la caracterización de las redes, topología y conceptos de protocolos y servicios. También se estudiarán las características generales de los modelos OSI y TCP/IP, así como el concepto de cableado estructurado.

Esta unidad es muy importante por todos los conceptos que se estudian en ella, ya que servirán de base a los conceptos que se estudiarán durante todo el módulo.

Al finalizar esta unidad serás capaz de caracterizar cualquier red según su topología, protocolos o tipos de cableado que utilice.

Recomendación

En éstos vídeos se hace una introducción, resumen y explicación de las partes más importantes de las 2 primeras unidades del curso.

Te recomiendo que los vayas viendo poco a poco, parándolo y volviendo a ver las partes que necesites conforme avances por el contenido.

<https://www.youtube.com/embed/bp1Tva1ryGY>

xjesus.net, Sesión Online 1 (CC BY-SA)

https://www.youtube.com/embed/_x3dobQHYDU

xjesus.net, Sesión Online 2 (CC BY-SA)

[Resumen textual alternativo para los vídeos de las Sesiones Online de introducción a las unidades 1 y 2](#)

Para saber más

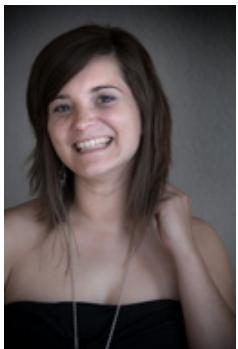
En Internet hay una gran cantidad de recursos que pueden ayudar a complementar estos materiales. Me gustaría destacar 2 por tener amplio material audiovisual y porque uno profundiza en lo teórico y otro en lo práctico:

- 1.- [Curso de redes de AulaClic](#) - Es un curso entero de redes de la Universidad Politécnica de Valencia, impartido por Rogelio Montañana y subido a Youtube por Aulaclic con su autorización. Se centra más en lo teórico que en lo práctico, de un nivel más alto que el exigido en el FP, pero el contenido merece mucho la pena, ya sea para ampliar información o por curiosidad. Los temas están muy bien explicados, y además son las grabaciones de clase, por lo que a veces hay preguntas de los alumnos y sus respuestas. Además está muy bien indexado, con lo que se puede tener una idea bastante clara del curso. Esa es la página con el índice y el acceso a todo el contenido, y también puedes ver [el enlace a su canal de Youtube](#).
- 2.- [Redes CCNA esencial](#) - Curso de Redes para ayudar a prepararse la certificación CCNA en Youtube. Más práctico con muchos ejemplos de Cisco Packet Tracer (la herramienta que usaremos para simular equipos de redes a lo largo del curso).

1.- Introducción y Terminología.

Caso práctico

Hace algunas semanas se han incorporado **Noiba**, **Naroba** y **Jana**, al departamento de Informática de **BK Sistemas Informáticos** para realizar el módulo de **FCT** del ciclo formativo de **ASIR**, y precisamente se han integrado en el equipo de trabajo que va a instalar una red local en el Aula de Formación de la empresa, tarea a cargo de **Laro** y **Vindio**, que precisamente serán los responsables del seguimiento de su formación en la empresa.



[Alain Bachellier \(CC BY-NC-SA\)](#)

Ellas han superado el módulo profesional de Planificación y Administración de Redes (PAR) y conocen toda la teoría necesaria para esta tarea, pero se encuentran algo indecisas sobre cómo empezar y se dejan llevar por las indicaciones de **Vindio**, quien les explica qué es lo que se espera de ellas, detallando las tareas y los plazos de realización de cada uno de ellos.

Antes de empezar **Jana** pregunta: "— ¿Qué tipo de red vamos a instalar y qué protocolos de comunicación utilizaremos?".

Todos la miran pensando que ha querido hacer la enterada.



[Alain Bachellier \(CC BY-NC-SA\)](#)

En esta unidad tomaremos contacto con el mundo de las redes de ordenadores, conoceremos sus características básicas, así como las diferentes técnicas utilizadas en su estudio.

Clasificación de las Redes.

Redes de difusión.

Redes punto a punto.

Redes LAN.

Redes MAN.

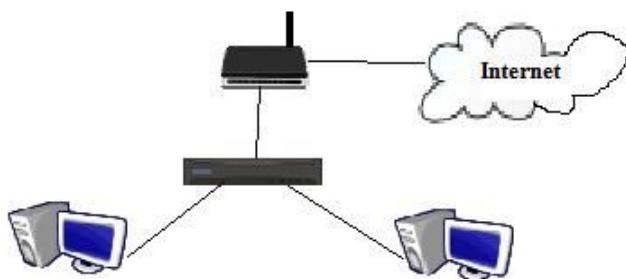
Redes WAN

Proyecto Opte.

Topologías.

Arquitectura.

Protocolos.



T. Fernández Escudero - Elaboración Propia. ([CC BY-SA](#))

1.1.- Clasificación de las Redes.

Las redes de ordenadores se pueden clasificar de acuerdo a varios criterios.

Los dos criterios más comunes son la extensión que ocupan todos sus elementos y la tecnología de transmisión. Pero también mediante otros criterios como son la topología, su titularidad, etc. como veremos en los siguientes subapartados.

Atendiendo a la tecnología de transmisión las redes se pueden clasificar en:

Redes de difusión.

Redes punto a punto.

Si lo que tenemos en cuenta es la extensión de la red, estas se pueden clasificar en:

Redes LAN.



T. Fernández Escudero-Elaboración Propia. ([CC BY-SA](#))

Redes MAN.



T. Fernández Escudero-Elaboración Propia. ([CC BY-SA](#))

Redes WAN.



T. Fernández Escudero-Elaboración Propia. ([CC BY-SA](#))

Autoevaluación

Las redes solo se pueden clasificar en función de su tecnología y extensión o tamaño.

Verdadero Falso

Falso

1.1.1.- Según Tecnología de transmisión.

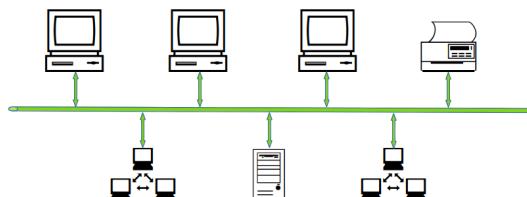
Redes de Difusión/broadcast (también llamadas multipunto o multidifusión)

Las redes de difusión son aquellas redes en las que se comparte un mismo canal de comunicación entre todos los nodos. Cuando uno de los nodos envía información, este tipo de redes tiene mecanismos para conseguir que aún compartiendo todos el mismo canal, la información llegue solamente al nodo al que va destinada.

Por ejemplo, cuando nosotros llamamos a una persona que se encuentra entre otras muchas, aunque todas oyen el mensaje, solamente nos contestará la persona requerida. En este caso, hemos compartido todos el mismo canal, pero hemos utilizado el nombre de esa persona para que la información sea solamente válida para ella, aunque todos los demás la han escuchado.

Esta tecnología no escala bien en redes grandes.

En la figura de abajo se puede ver como eran las LAN originalmente con un cable compartido que sería lo equivalente a tener hoy en día un **concentrador (o hub)**.



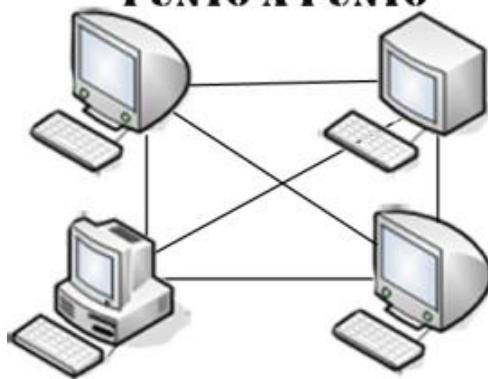
Alfonso Bonillo - Elaboración propia. ([CC BY-SA](#))

Redes punto a punto

Las redes "punto a punto", como su propio nombre nos puede indicar, son redes en las que existen multitud de conexiones entre pares individuales. En este caso no se comparte canal y puede haber muchas rutas. Esta tecnología es la causante del gran éxito de aplicaciones con Emule, aplicaciones que sirven para intercambiar datos entre dos personas. A veces se les asigna el nombre de "p2p" o "peer to peer".

Este tipo de redes escalan mejor para redes grandes, y a día de hoy prácticamente todas las redes son así. Por ejemplo a nivel de LAN se usan **comutadores (o switches)** que establecen conexiones punto a punto con todos sus equipos conectados de forma que se aprovecha mucho mejor el ancho de banda.

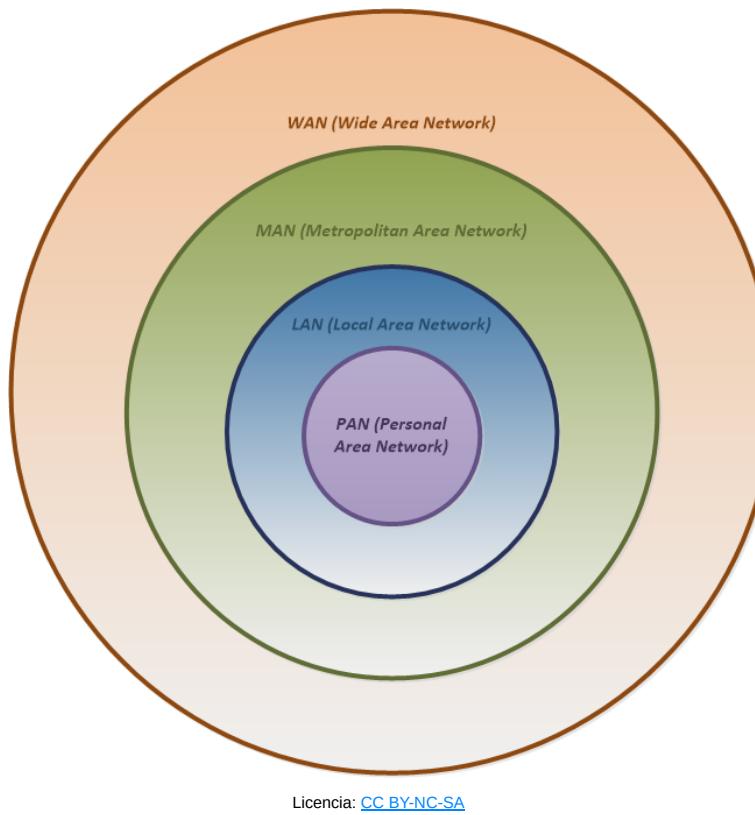
PUNTO A PUNTO



[Adonis Rojas Madrigal \(CC BY-SA-4.0\)](#)

1.1.2.- Según la extensión o tamaño de la red.

La localización geográfica de la red es un factor a tener en cuenta a la hora de diseñarla y montarla. No es lo mismo montar una red para un aula de informática que interconectar las oficinas de dos sucursales que la misma empresa tiene instalada en diferentes países. Sin embargo, esta clasificación resulta confusa o arbitraria, ya que se basa en criterios vagamente definidos.



Subred o segmento de red: Un segmento de red está formado por un conjunto de ordenadores o estaciones de trabajo que comparten el mismo medio de transmisión (normalmente conectados con el mismo cable). El segmento está limitado en espacio al departamento de una empresa, un aula de informática etc. Se considera el segmento como la red de comunicación más pequeña, y todas las redes de mayor tamaño están constituidas por la unión de varios segmentos de red.

Red de área local o Local Area Network (LAN): Una red de área local es un sistema que permite la interconexión de equipos informáticos que están próximos físicamente. Entendemos por próximo todo lo que no sea cruzar una vía pública: una habitación, un edificio, un campus universitario, etc.

En el momento en que una red debe cruzar una calle, o una vía pública en general, es preciso que una compañía de telecomunicaciones establezca la comunicación, puesto que son las únicas autorizadas para pasar líneas por zonas públicas.

Otra definición más precisa de red de área local, prescinde de la distancia entre las estaciones y especifica que su carácter distintivo reside en que los mecanismos de enlace entre estaciones deben estar completamente bajo el control de la persona o entidad que establece dicha red.

Por lo tanto, podemos considerar el término red local como un término vago que se refiere a uno o varios segmentos de red conectados mediante dispositivos especiales.

Generalmente se encuentran en su totalidad dentro del mismo edificio o grupo de edificios. Van desde unos pocos metros a unos pocos kilómetros.

Las redes locales supusieron una solución al crecimiento de soluciones de redes totalmente incompatibles planteadas por distintos fabricantes. Las tecnologías que implementaron permitieron conectar de forma eficiente equipos informáticos tales como las estaciones de trabajo, dispositivos periféricos, terminales y otros dispositivos ubicados dentro de un mismo edificio.

Sus principales características son:

Tamaño: Restringidas a un edificio, planta edificio, campus. De 10m a 1Km.

Topología: Bus, estrella y anillo.

Tasa de transferencia: Relativamente elevada (de 10Mbps a 10Gbps). La tasa de transferencia es la velocidad de transmisión de una señal. Se mide en bits por segundo (bps).

Tecnología: Medio de transmisión como el par trenzado y la fibra óptica. Incluso medios inalámbricos en forma de ondas de radio. El medio suele ser compartido aunque últimamente se emplean técnicas de conmutación con los medios cableados para mejorar su rendimiento.

Tasa de errores: Fiables, muy seguras y con pocos errores.

Privacidad: Toda la red pertenece a la misma organización.

Aplicaciones: Las mismas que las redes en general.

Las LANs mas conocidas y extendidas son la Ethernet, Token Ring , LAN inalámbrica, etc.

Red de Campus: Se extiende entre varios edificios dentro de un mismo polígono industrial que se conectan generalmente a un tendido de cable principal. Normalmente, la empresa es propietaria del terreno por el que se extiende el cable y tiene libertad para poner cuantos cables sean necesarios sin tener que solicitar permisos especiales.

Red de área metropolitana o Metropolitan Área Network (MAN): Generalmente está confinada dentro de una misma ciudad y se haya sujeta a regulaciones locales. Puede constar de varios recursos públicos o privados, como el sistema de telefonía local, sistemas de microondas locales o cables enterrados de fibra óptica (redes de cable). Una empresa local construye y mantiene la red, y la pone a disposición del público. Puede conectar sus redes a la MAN y utilizarla para transferir información entre redes de otras ubicaciones de la empresa dentro del área metropolitana.

Las MAN más conocidas son la FDDI, ATM, Wimax (Inalámbrica)

Red de área extensa o Wide Área Network (WAN): A medida que el uso de los ordenadores en las empresas aumentaba, pronto resultó obvio que incluso las redes locales (LAN) no eran suficientes. En un sistema LAN, cada departamento o empresa, era una especie de isla electrónica.

Se necesitaba que la información se pudiera transferir rápidamente y con eficiencia, no solamente dentro de una misma empresa sino de una empresa a otra. La solución fue la creación de redes de área metropolitana (MAN) y redes de área amplia (WAN). Como las WAN podían conectar redes de usuarios dentro de áreas geográficas extensas, permitieron que las empresas se comunicaran entre sí a través de grandes distancias

Una red de área extendida (WAN) abarca varias ciudades, regiones o países. Los enlaces WAN son ofrecidos generalmente por empresas de telecomunicaciones públicas o privadas que utilizan enlaces de fibra óptica, microondas o vía satélite. Actualmente, el método empleado para conectar una WAN utiliza líneas telefónicas estándar o líneas telefónicas modificadas para ofrecer un servicio más rápido.

Las WAN mas conocidas son ofrecidas por las compañías telefónicas (Movistar,..), redes de cable (ONO,...), redes de telefonía móvil (Movistar, Vodafone, Orange,...), enlaces vía satélite, etc.

También podríamos añadir a nuestra clasificación otros tipos de redes como son los siguientes:

Red de área personal o Personal Área Network (PAN): Incluye el entorno de usuario (PC, PDA, Pocket PC, Móvil, Ipod, portátiles, Tablets, Palms, etc). Normalmente son redes inalámbricas que utilizan tecnologías bluetooth o infrarrojos...

Red de área local inalámbricas o wireless local área network (WLAN): Representan otra mejora importante de las redes locales (cableadas) en las que el enlace entre equipos informáticos no se lleva a cabo por medio de cables, sino por medio de enlaces radioeléctricos (ondas de radio). Las ventajas de este tipo de enlaces, en cuanto a movilidad y facilidad de instalación, son evidentes.

Las WLAN mas conocidas son las redes Wifi e incluso la Wimax.

Autoevaluación

Las redes se clasifican en LAN, MAN y WAN de acuerdo a:

Sugerencia

- El tipo de interconexiones que utilizan, modem para las LAN y router para las MAN y WAN.
-

1.1.3.- Según su titularidad.

Esta clasificación atiende a la propiedad de la red: redes privadas dedicadas y redes compartidas.



[Mykel](#)

Redes dedicadas o privadas: Tienen un propietario no público. Todo su recorrido es propiedad del poseedor de la red. También puede ocurrir que determinadas redes sean alquiladas a compañías de comunicaciones (públicas o privadas) para su uso exclusivo.

públicas: Son redes de titularidad pública. Normalmente en poder de compañías telefónicas (como Movistar) o de cable (como ONO). Las líneas de comunicación soportan información de diferentes usuarios. Se trata en todo caso de redes de servicio público ofertadas por compañías de telecomunicaciones bajo cuotas de alquiler en función de la utilización realizada. Pertenece a este grupo la redes telefónicas comutadas y las redes especiales para transmisión de datos (Telefónica / Movistar, Vodafone, ONO, etc.).

Autoevaluación

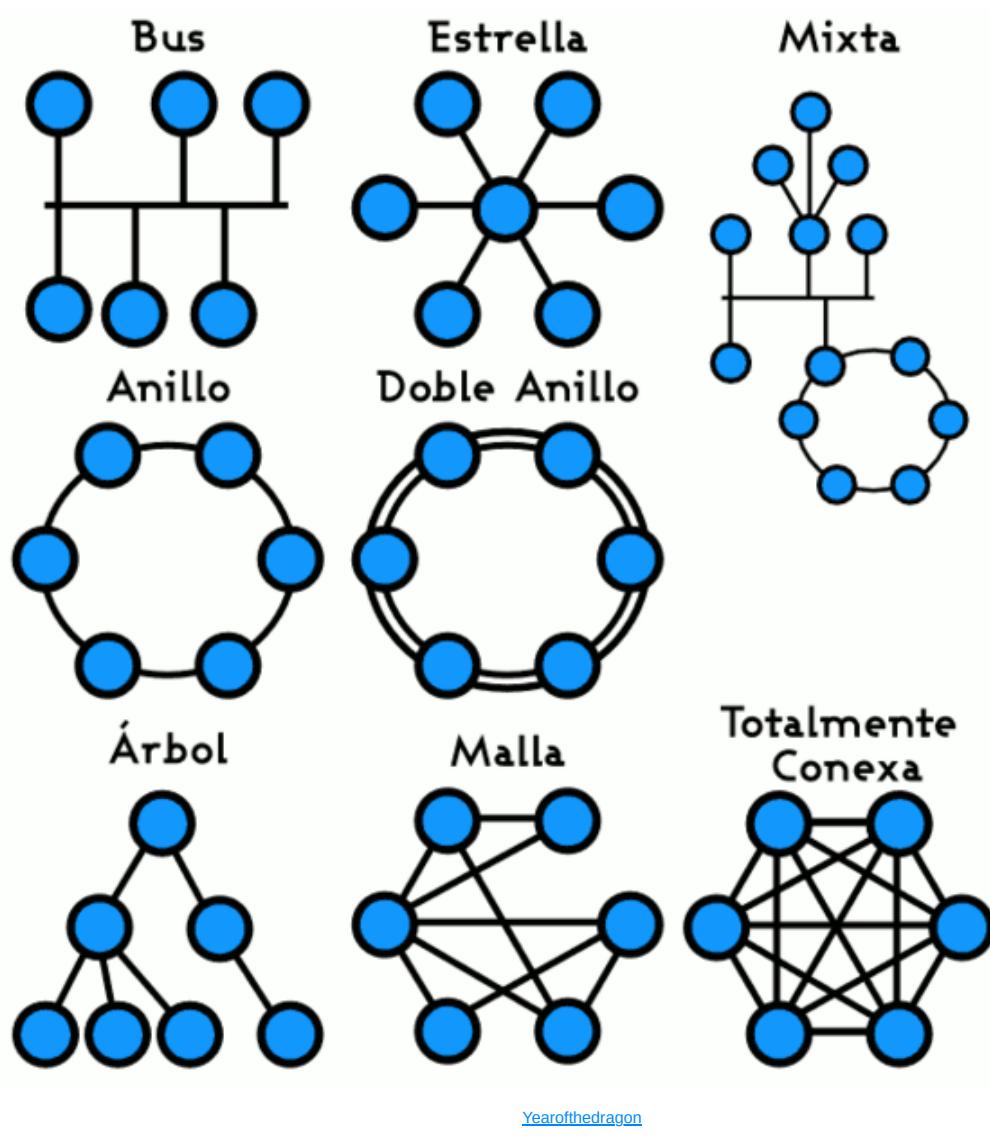
Si la red de tu casa o empresa usa un router de un proveedor como Movistar por ejemplo, entonces ¿es una red pública?

[Sugerencia](#)

Verdadero Falso

Falso

1.1.4.- Segú su topología.



específicos.

Bus: Utiliza un único cable para conectar los equipos. Esta configuración es la que requiere menos cableado, pero tiene el inconveniente de que, si falla algún enlace, todos los nodos quedan aislados.

Árbol: Es una forma de conectar nodos como una estructura jerarquizada. Esta topología es la menos utilizada, y se prefiere la topología irregular, ya que el fallo de un nodo o enlace deja al conjunto de nodos incomunicados entre sí.

Anillo: Todos los nodos están conectados a una única vía con sus dos extremos unidos. Al igual que ocurre con la topología en bus, si falla algún enlace, la red deja de funcionar completamente.

Irregular: Cada nodo debe estar conectado, como mínimo, por un enlace, pero no existen más restricciones. Esta topología es la más utilizada en redes que ocupan zonas geográficas amplias.

Esta clasificación tiene en cuenta la arquitectura de la red, es decir, la forma en la que se interconectan los diferentes equipos informáticos o usuarios a ella:

Malla: Es una interconexión total de todos los nodos, con la ventaja de que, si una ruta falla, se puede seleccionar otra alternativa. Este tipo de red es más costoso de construir ya que hace falta más cable.

Estrella: Los equipos se conectarán a un nodo central con funciones de distribución, commutación y control. Si el nodo central falla, quedará inutilizada toda la red; si es un nodo de los extremos, sólo éste quedará aislado. Normalmente, el nodo central no funciona como estación sino que más bien suele tratarse de dispositivos

Autoevaluación

Si tenemos 3 PCs conectados a un switch o a un router, ¿se dice que es una topología en estrella?

- Verdadero Falso

Verdadero

1.1.5.- Según la forma de transferencia de la información

Esta clasificación tiene en cuenta la técnica empleada para transferir la información desde el origen al destino. Por lo tanto, también depende de la topología de la red y, si se ha separado de la clasificación anterior, ha sido porque existen diferentes topologías que comparten el mismo método de transmisión.

Redes conmutadas (punto a punto): En este tipo de redes, un equipo origen (emisor) selecciona un equipo con el que quiere conectarse (receptor) y la red es la encargada de habilitar una vía de conexión entre los dos equipos. Normalmente pueden seleccionarse varios caminos candidatos para esta vía de comunicación que puede o no dedicarse exclusivamente a la misma. Existen tres métodos para la transmisión de la información y la habilitación de la conexión:

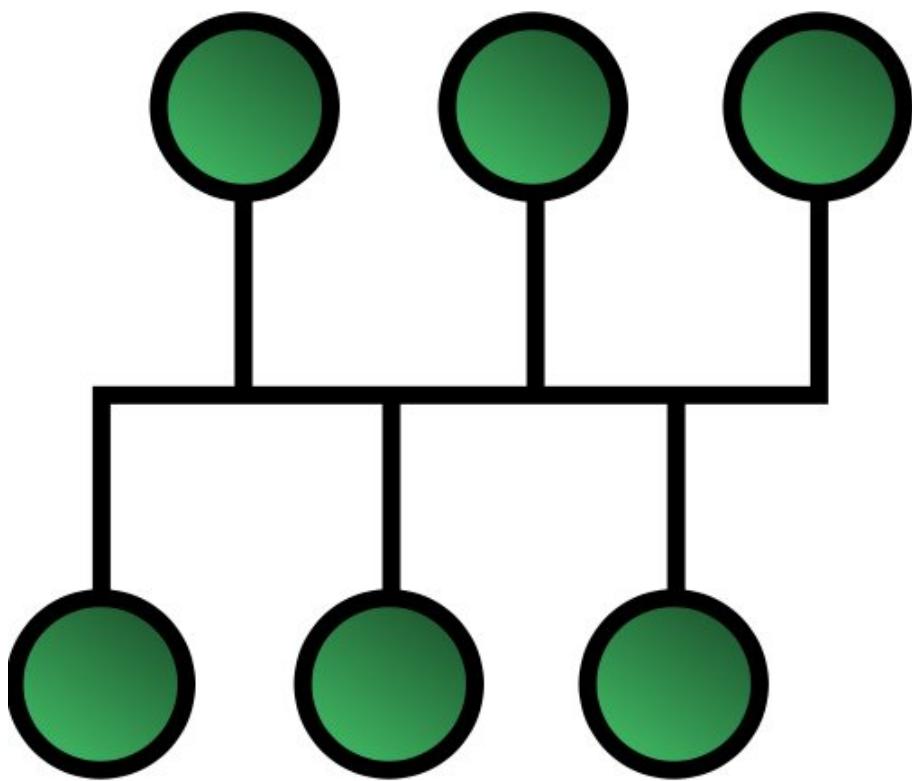
Conmutación de circuitos: Se establece un camino dedicado. La ruta que sigue la información se establece durante todo el proceso de conexión, aunque existan tramos de esta ruta que se comparten con otras rutas diferentes. Una vez finalizada la comunicación, es necesario liberar la conexión.

Conmutación de paquetes: En este caso, el mensaje a enviar se divide en fragmentos, cada uno de los cuales es enviado a la red y circula por ésta hasta que llega a su destino. Cada fragmento denominado paquete, contiene parte de la información a transmitir, información de control además de los números o direcciones que identifican el origen y el destino.

Conmutación de mensajes: La información que envía el emisor se aloja en un único mensaje con la dirección de destino y se envía al siguiente nodo. Éste almacena la información hasta que hay un camino libre, dando lugar a su vez al envío al siguiente nodo hasta que finalmente llegue al destino.

[Myself](#)

Redes de difusión (multipunto o broadcast): En este caso un equipo o nodo envía la información a todos los equipos y es el destinatario el encargado de seleccionar y captar esa información. La red debe tener una topología en bus o anillo o debe estar basada en enlaces por ondas de radio.



[Myself](#)

Página 8 de 83

1.1.6.- Según su relación funcional.

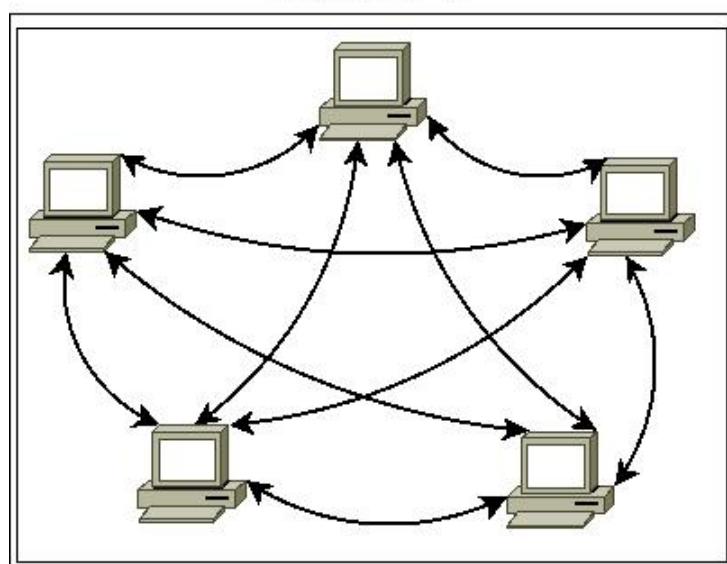
La principal función de las redes consiste en que los ordenadores de la red puedan compartir recursos entre todos los usuarios autorizados del sistema, mediante el intercambio de tramas de datos entre los distintos equipos conectados a las líneas de transmisión.

La capacidad ofrecida por un ordenador a otros en una red se llama servicio o recurso. Los ordenadores que usan un servicio se llaman clientes y los que lo ofrecen se denominan servidores.

Hay dos maneras fundamentales de establecer la conexión de los ordenadores en la red según la ubicación de los recursos.

Redes ENTRE IGUALES o Peer to Peer (P2P): Cualquier ordenador puede ser cliente y/o servidor. No está claramente definida tal función. Todos los ordenadores ponen a disposición de los demás los recursos que disponen, fundamentalmente discos e impresora. Esta estructura es muy simple pero se hace difícil el control de los recursos.

Modelo P2P



[Alancaio](#)

Redes CLIENTE-SERVIDOR: En este tipo de distribución está claramente definido los ordenadores que son servidores y cuáles clientes. En este caso se privilegia a uno o varios ordenadores confiriéndoles capacidades añadidas en forma de servicios, denominándose servidores o servers. El resto de los ordenadores solicitan servicios a estos servidores que estarán altamente especializados en la función para la que fueron diseñados creando así una estructura centralizada. Este tipo de organización es mucho mas fácil de administrar.

[Alancaio](#)

Ejemplos de servidores: Impresión, discos (o ficheros), aplicaciones, web, correo electrónico, fax, etc. Incluso podemos considerar redes híbridas donde se combina los dos modelos anteriores.

Autoevaluación

¿Las páginas web funcionan mediante P2P?

- Verdadero Falso

Falso

Funcionan mediante una relación de cliente (aplicación de navegador web como Chrome en un PC) que se conecta a un servidor de páginas web escritas en lenguaje HTML y usando el protocolo HTTP para la conexión entre cliente y servidor.

1.2.- Elementos de una red.

Para construir una red local, se precisan básicamente dos cosas:

Elementos físicos o hardware: Está formado por equipos informáticos (ordenadores y dispositivos de naturaleza variada) y medios de transmisión que posibilitan implementación física de la red. Como ejemplo tendríamos ordenadores, estaciones de trabajo, servidores, tarjeta de red, módem, dispositivos de interconexión, dispositivos de impresión, cables, etc.

Elementos lógicos o software: Ofrece las capacidades necesarias para que los usuarios y sus aplicaciones puedan acceder y utilizar los recursos o servicios de la red. Normalmente estas capacidades se integran en forma de programas en los propios sistemas operativos. Tampoco podríamos olvidar los propios recursos o servicios como por ejemplo las aplicaciones de red, los datos, los mensajes, etc.

A modo de ejemplo describimos algunos elementos que podemos encontrarnos en una red:

Dispositivos finales: La mayoría de los componentes de una red media son los ordenadores individuales, también denominados host; generalmente son sitios de trabajo o servidores. Cada ordenador conectado a la red conserva la capacidad de funcionar de manera independiente, realizando sus propios procesos. Asimismo, los ordenadores se convierten en estaciones de trabajo en red, con acceso a la información y recursos contenidos en el servidor de archivos de la misma. Una estación de trabajo no comparte sus propios recursos con otros ordenadores.



[ISFTIC](#)

Servidores: Son también dispositivos finales. Son aquellos ordenadores capaces de compartir sus recursos con otros. Los recursos compartidos pueden incluir impresoras, unidades de disco, CD-ROM, directorios en disco duro e incluso archivos individuales. Los tipos de servidores obtienen el nombre dependiendo del recurso que comparten. Algunos de ellos son: servidor de discos, servidor de archivos, servidor de archivos distribuido, servidores de archivos dedicados y no dedicados, servidor de terminales, servidor de impresoras, servidor de discos compactos, servidor web, servidor de correo, etc.

Medio de transmisión: La LAN debe tener un sistema de cableado que conecte las estaciones de trabajo individuales con los servidores de archivos y otros periféricos. Si sólo hubiera un tipo de cableado disponible, la decisión sería sencilla. Lo cierto es que hay muchos tipos de cableado, cada uno con sus propios defensores y como existe una gran variedad en cuanto al costo y capacidad, la selección no debe ser un asunto trivial. Ejemplos de cables usados en las redes locales son el par trenzado, coaxial y fibra óptica. Tampoco debemos olvidar el desarrollo de los medios de transmisión sin cables (inalámbricos).

Dispositivos intermedios: También conocidos como dispositivos de interconexión. Se encargan de implementar el direccionamiento y administración de los mensajes en la red de forma que los

equipos informáticos se puedan comunicar entre sí. Ejemplos de dispositivo de interconexión son los hubs, switches, routers, etc.

Tarjeta de interfaz de red o Network Interface Card (NIC): Para comunicarse con el resto de la red, cada ordenador debe tener instalado una tarjeta de interfaz de red. Se les llama también adaptadores de red o sólo tarjetas de red. En la mayoría de los casos, la tarjeta se adapta en la ranura de expansión de la computadora, aunque algunas son unidades externas que se conectan a ésta a través de un puerto USB. La tarjeta de interfaz obtiene la información del PC, la convierte al formato adecuado y la envía a través del medio de transmisión a otra tarjeta de interfaz de la red local. Esta tarjeta recibe la información, la traduce para que el PC pueda entenderla y la entrega al PC.



[Wikipedia](#)

Software base: También conocido como **Sistema operativo de red o Network operating system (NOS)**: Después de cumplir todos los requerimientos de hardware para instalar una LAN, se necesita instalar un sistema operativo de red, que administre y coordine todas las operaciones de dicha red. Los sistemas operativos de red tienen una gran variedad de formas y tamaños, debido a que cada organización que los emplea tiene diferentes necesidades. Algunos sistemas operativos se comportan excelentemente en redes pequeñas, así como otros se especializan en conectar muchas redes pequeñas en áreas bastante amplias. Ej: Windows 7.

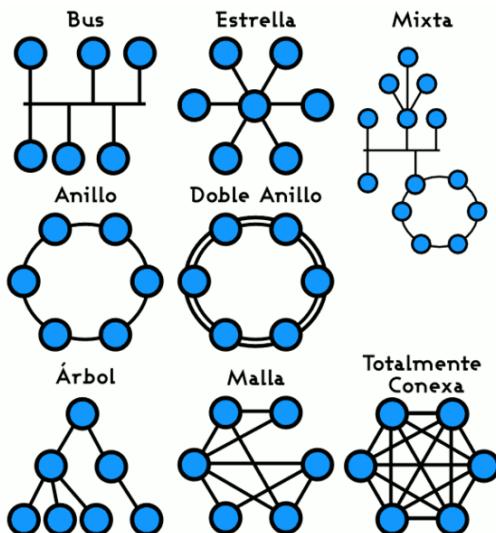
Software de aplicación: Son el conjunto de programas a través de los cuales los usuarios utilizan los recursos de la red tanto locales como remotos. Este software puede ser tan amplio como se necesite ya que puede incluir procesadores de texto, hojas de cálculo, clientes de correo electrónico, etc. Ej: Internet Explorer.

1.3.- Topologías, arquitectura y protocolos.

Topologías

La topología de red se define como la cadena de comunicación usada por los nodos que conforman una red para comunicarse. La topología se puede referir tanto al camino físico como al lógico.

Las principales topologías de red son bus, estrella, anillo y malla. Internet es un claro ejemplo de malla. La topología es uno de los criterios que se pueden tener en cuenta si queremos clasificar una red.



[Yearofthedragon-Wikimedia \(CC BY-SA-3.0\)](#)

Un tipo de topología muy común es la topología en estrella, un elemento sirve para interconectar los demás nodos de la red, por ejemplo, varios ordenadores unidos entre sí mediante un switch o router. En las redes de tipo LAN se suele seguir este tipo de topología.

Autoevaluación

Cuando todos los elementos que forman parte de una red están unidos entre sí a través de otro nodo central se dice que esa red tiene una topología:

- En anillo porque si elimino uno de los nodos se rompe la comunicación en toda la red.
- En bus.
- Física en estrella.
- Lógica en anillo.

No es correcto. En anillo la topología es circular conectando cada nodo con el siguiente.

No es correcta. La topología en bus consiste en que todos comparten un mismo canal.

Correcto. Puede ser lógica o física, el aspecto físico nos da detalles para asegurar una topología física.

NO es correcta. La topología en anillo, ya sea lógica o física, es circular.

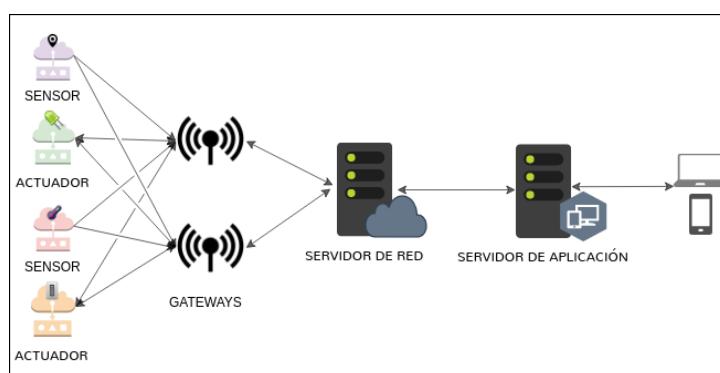
Solución

1. Incorrecto
2. Incorrecto
3. Opción correcta
4. Incorrecto

Arquitectura

La arquitectura de una red es el conjunto de elementos, normas, protocolos, estándares y todo lo necesario para poder definir un determinado tipo de red. De igual modo que podemos clasificar los edificios por los materiales utilizados, el tamaño, la forma, el color, también lo podemos hacer en las redes informáticas por su arquitectura.

Las principales arquitecturas son las arquitecturas de niveles, capas y protocolos OSI y TCP/IP. El principal cometido de una arquitectura es el poder separar las funciones de cada uno de los elementos que intervienen en una red. Por ejemplo, por un lado se gestionan los componentes físicos, por otro lado el software de base y por último las aplicaciones de usuario, esto sería un ejemplo de una arquitectura de red de tres niveles.



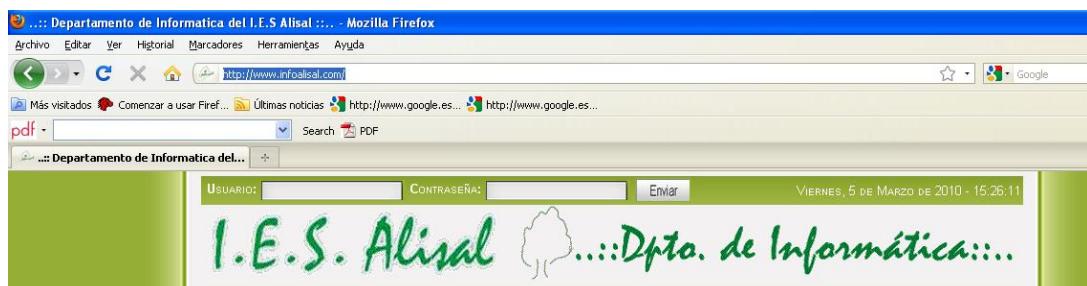
[Brivadeneira-Wikimedia \(CC BY-SA\)](#)

Protocolos

Los protocolos son las normas que se deben cumplir, tanto a nivel lógico como físico para que una red funcione. Son las reglas necesarias para que la red funcione como tal. Ejemplos de protocolos son:

Ethernet,
Fast Ethernet,
Gigabit Ethernet,
Token Ring,
FDDI,
ATM,
HDLC,
IP,
TCP,
UDP,
FTP,
HTTP,
Telnet,
SSH,
POP3,
SMTP,
IMAP,
PPP.

Cada protocolo es válido para un determinado nivel; HTTP es el protocolo (entre otros más) que nos permite visualizar una página web en nuestro navegador.



T. Fernández Escudero-Elaboración propia ([CC BY-SA](#))

1.4.- El sector de las redes y sus actores principales.

El sector o la industria de las redes es un sector muy dinámico y competitivo, con grandes oportunidades de negocio y de empleo para un técnico de redes.

A grandes rasgos se puede hablar que por un lado están los **Organismos de Estandarización (ISO, IEEE, ANSI, IETF, etc.)** que son organismos supra-nacionales, continentales o internacionales en general dónde se debaten, definen y revisan las normas, estándares y protocolos de redes que los **fabricantes de equipos de redes** implementarán y desarrollarán. Aunque en muchas ocasiones hay una estrecha colaboración o incluso algunos fabricantes crean estándares "**de facto**" que posteriormente son estandarizados por algún organismo.

Los **fabricantes**, para poder llegar a vender e instalar sus equipos a nivel mundial y local se sirven de **Socios integradores (Partners)** que ofrecen la experiencia, servicio de consultoría, diseño, implementación y soporte post-venta a sus **clientes**, asociándose con varios fabricantes especializados en distintas tecnologías para ofrecer **soluciones "llave en mano"**.

Las empresas fabricantes de equipos de redes suelen distinguir entre sus **clientes**, a grandes rasgos, en **3 segmentos** principales de comercialización:

Doméstico o [PYMEs](#) (Pequeñas y medianas empresas) o en inglés **SOHO** (Small Office Home Office)

Empresarial o en inglés **Enterprise**, para empresas de más de 200 empleados o con una gran carga de tráfico digital.

Proveedor de Servicios de Internet o en inglés **ISP** (Internet Service Provider), para empresas que se dedican a dar servicios de Internet como Movistar, Vodafone, Orange, etc. con miles de clientes (domésticos, PYMES o Empresariales igualmente).

En el ámbito doméstico y [PYMEs](#) (como clientes de las redes de los [ISP](#)), se han usado todo tipo de routers (o encaminadores) de distintas compañías. Una de las destacadas es **Linksys**, famosa por haber desarrollado uno de los routers con más éxito comercial, el [WRT54G](#), gracias a que tenía un firmware basado en GNU/Linux con un interfaz de gestión web muy potente e intuitivo, pero que por cumplir la licencia GPL se vieron obligados a publicar su código fuente, logrando para su sorpresa convertirse en top ventas. Al hacerse libre su firmware, fue posible para una gran comunidad de entusiastas añadirle nuevas funcionalidades para conseguir hacer cosas sólo disponibles en equipos mucho más caros (empresariales) como QoS (para limitar el ancho de banda), VoIP, VPN, firewall, proxy, VLANs, configuraciones avanzadas de WiFi y seguridad, clientes de Emule, BitTorrent, servidores de medios DLNA, FTP, etc.

Existen varios proyectos de desarrollo que proveen versiones mejoradas del firmware para equipos domésticos como el WRT54G y similares:

[DD-WRT](#)
[OpenWrt](#)
[Tomato](#)

Estos firmwares se han portado a otros equipos de otras marcas con hardware similar gracias a la facilidad de integrar sus drivers en el núcleo Linux.

Algunas de las compañías **fabricantes** produciendo equipos en el segmento doméstico y PYMEs son ASUS, D-Link, TP-Link, Netgear, Belkin, Xiaomi o Huawei.

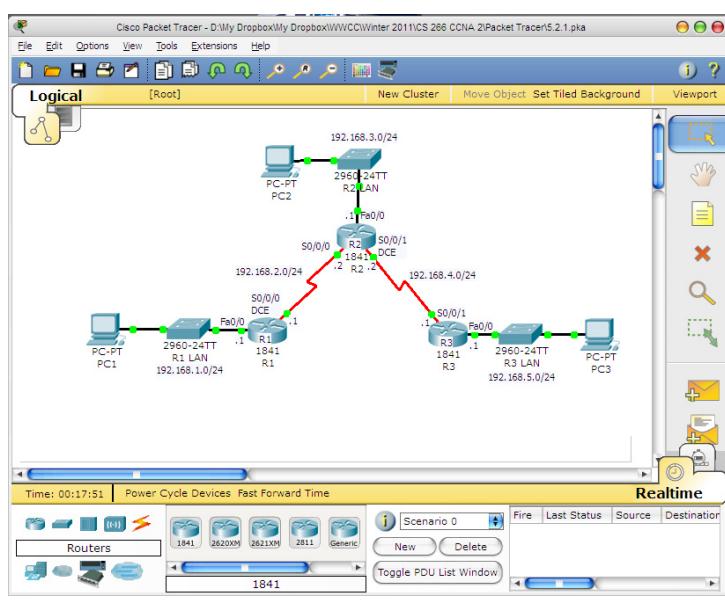
[chrandcamver, Routers Cisco \(CC BY\)](#)

Sin embargo, desde los inicios del sector de las redes, la compañía con más ventas de routers en el **segmento empresarial e ISP** ha sido **Cisco Systems**, que en 2003 adquirió Linksys para intentar entrar en el segmento SOHO para posteriormente en 2013 venderla a Belkin.

Los routers Cisco, tanto los más pequeños como los más grandes, en general han funcionado con un sistema operativo llamado **IOS (Internet Operating System)**, no confundir con el sistema operativo del iPhone que fue posterior y requirió el permiso de Cisco) y han marcado una especie de estándar de facto en la industria a la hora de usar los comandos de gestión de los routers.

Tradicionalmente los routers se han configurado mediante comandos en una consola de texto (CLI o interfaz de línea de comandos) accediendo a través de un puerto serie (ahora también USB o Universal Serial Bus), o en remoto mediante telnet o ssh. Aún a día de hoy sigue siendo la forma más óptima y útil de acceder a toda la funcionalidad y de poder realizar **scripts** de configuración de múltiples equipos a la vez. Por eso es conveniente conocer estos comandos, incluso aunque últimamente también sea posible gestionarlos mediante interfaz gráfica web en ciertos casos.

A partir de la unidad 3 se verán estos comandos en un simulador de routers Cisco llamado Packet Tracer.



[goblinbox, Cisco Packet Tracer \(CC BY\)](#)

Por citar a otras compañías, en el segmento ISP o de grandes empresas, la competencia de Cisco siempre ha sido Juniper y más recientemente Huawei, con equipos muy similares a los de Cisco (con los mismos comandos de IOS, e incluso los mismos bugs, llevándoles a juicio...) pero a precios más competitivos. Cisco perdió mucho mercado de exportaciones tras conocerse el uso de puertas traseras en los equipos de todos los fabricantes americanos para dar acceso a la NSA.

Por otro lado, las funcionalidades de un router también se han podido realizar mediante ordenadores personales (PCs) con una o varias tarjetas de red cableadas y/o inalámbricas, normalmente corriendo Unix/Linux por rendimiento, aunque también es posible hacerlo con Windows. Por ejemplo mediante proyectos con software libre como Zebra y Quagga que ahora han evolucionado a: <https://frrouting.org/>

Autoevaluación

¿Cisco es un organismo de estandarización?

- Verdadero Falso

Falso

Es un fabricante de equipos de redes y desarrollador de software para redes. Aunque igualmente colabora con los organismos de estandarización (y con otros fabricantes) a sacar nuevos estándares.

1.4.1.- Normas y asociaciones de estándares.

A partir de entonces, se comprobó que era necesario definir un conjunto común de normas que permitieran coordinar a todos los fabricantes.

El proceso de comunicación requiere que los distintos fabricantes, organismos internacionales y estados se pongan de acuerdo en el modo que se llevará a cabo la comunicación. Para ello se establecen una serie de normas o estándares.

Los estándares pueden ser de dos tipos:

De facto o de hecho: Aceptado en el mercado por su uso generalizado. Tenemos algunos ejemplos como el ordenador personal o PC de IBM, el sistema operativo UNIX o los protocolos TCP/IP.

De iure o de derecho: Estándar propuesto por una asociación de estándares que se propone a los fabricantes.

Tenemos algunos ejemplos de ambos tipos:

ITU (Unión Internacional de comunicaciones): Es el nombre actual del antiguo CCITT. Se encarga de realizar recomendaciones técnicas sobre teléfonos, telégrafo y comunicaciones de datos. Ejemplos: recomendación V.24 o EIA 232/RS 232, Serie V(V.32, V.34, V.90, V.92,), Serie X sobre redes de datos (X.25, X.400), RDSI (Acceso Básico y Acceso Primario), RDSIBA (ATM FORUM), etc.

ISO (Organización Internacional para Estandarización): Regula aspectos sobre la red de fibra óptica FDDI, el modelo de comunicaciones OSI, comunicaciones e interconexión de redes, sistemas de gestión de calidad, etc.

ANSI: Miembro de OSI. Trabaja con empresas americanas. Trabaja con características de monitores, telecomunicaciones digitales, fibra óptica (FDDI), etc.

IEEE (Institute of Electrical and Electronics Engineers): Se ocupan de aspectos acerca del funcionamiento de las redes locales (LAN) a través de los estándares 802.

Internet Society (ISOC): Absorbió a la Internet Association Board (IAB). Se encarga de supervisar la aparición de nuevos estándares y protocolos para internet. Los acuerdos aparecen publicados en unos documentos denominados RFC (Request for comments).

La Internet Society es la organización que provee la infraestructura corporativa, así como el financiamiento, apoyo jurídico y fiscal de la Internet Engineering Task Force (IETF). Anualmente ISOC aporta a la IETF alrededor de un millón de dólares para la elaboración de los Requests for Comments (RFC editor), considerados los estándares de Internet que se determinan mediante equipos de trabajo que operan de manera abierta y democrática para asegurar la evolución transparente de Internet. La IETF ofrece una vasta variedad de publicaciones que incluyen una serie de resúmenes diarios y semanales sobre temas actuales y desarrollos de los estándares propuestos, protocolos y tópicos relacionados.

ICANN (Internet Corporation for Assigned Names and Numbers) e **IANA** (Internet Assigned Numbers Authority). Su función principal consiste en mantener un registro central de números asociados con los protocolos de internet, además de los nombres de dominio y direcciones de red.

Para saber más

Puedes consultar los proyectos y grupos de trabajo de las distintas organizaciones de estandarización:

[ITU](#)

[ISO](#)

[IEEE](#)

[ISOC](#)

[ICANN](#)

En esta web se describen y resumen muy bien las organizaciones de Estándares:
<https://ccnadesdecero.es/organizaciones-estandares/>

Autoevaluación

¿Unix y TCP/IP son estándares "de facto"?

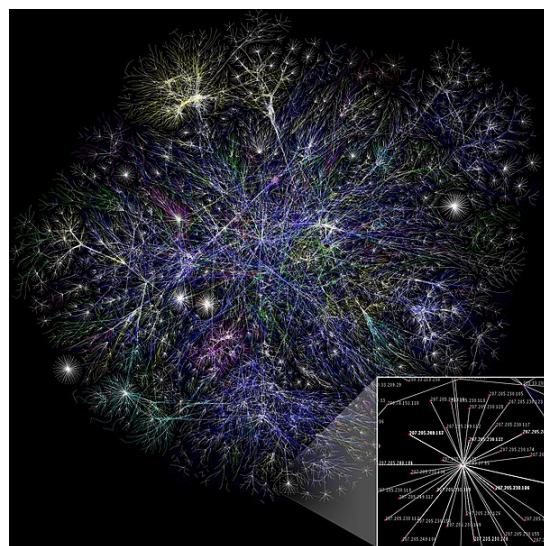
[Sugerencia](#)

Verdadero Falso

Verdadero

1.5.- Proyecto Opte: Representando Internet en tiempo real.

El proyecto **Opte** tiene como objetivo representar en tiempo real todas las conexiones que forman Internet. Si representásemos todas las conexiones entre ordenadores servidores que existen y dan vida a Internet nos quedaría algo similar a lo que representa la siguiente figura:



[The Opte Project - Wikimedia \(CC BY\)](#)

La imagen representa un mapa parcial de Internet basado en la información obtenida del sitio "opte.org" el 15 de enero de 2005. Cada línea dibujada entre dos nodos representa el enlace entre dos direcciones IP. La longitud de las líneas es proporcional al tiempo de espera entre los nodos. La imagen representa 30% de las redes tipo C accesibles en 2005. El color de las líneas corresponde a una distribución según la siguiente lista:

- Azul oscuro: net, ca, us
- Verde: com, org
- Rojo: mil, gov, edu
- Amarillo: jp, cn, tw, au, de
- Magenta: uk, it, pl, fr
- Dorado: br, kr, nl
- Blanco: desconocido

Cada color representa las redes pertenecientes a los dominios de Internet net, ca, us com, org mil, gov, edu, jp, cn, tw, au de, uk, it, pl, fr br, kr, nl.

net, ca, us com, org mil, gov, edu, jp, cn, tw, au de, uk, it, pl, fr, br, kr, nl

Para saber más

Si quieres profundizar tus conocimientos sobre este proyecto, te recomendamos visitar el siguiente artículo de la Wikipedia.

[El Proyecto de Mapeo de Internet.](#)

También tienes más información en el siguiente artículo en inglés.

[The Internet Map.](#)

Si quieres saber más sobre la historia de la red de redes: internet

[¿Qué es Internet?](#)

2.- Sistemas de numeración y unidades.

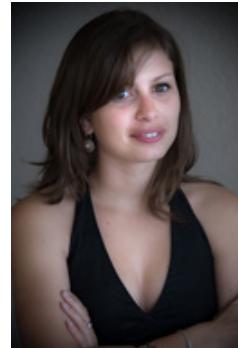
Caso práctico



[Alain Bachellier \(CC BY-NC-SA\)](#)

Tras unos días trabajando en la instalación de la red local, **Naroba** comenta a **Noiba** lo increíble que resulta entender la transferencia de la información en una red, ya sea cableada o inalámbrica.

Desde documentos de texto a imágenes, pasando por audios o vídeos, cualquier cosa se puede compartir a través de una red, algo que ha cambiado la forma de trabajar en empresas de todos los sectores productivos. Y todo ello se reduce a la transferencia de bits, que representamos con lo más simple que conocemos; ceros y unos.



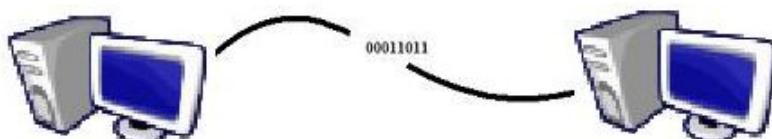
[Alain Bachellier \(CC BY-NC-SA\)](#)

Noiba añade que aún puede entender la transmisión de datos a través de una red cableada mediante pulsos eléctricos, pero no es fácil de asimilar que circulen por el aire de forma ordenada con múltiples redes compartiendo el medio.

Información es todo aquello que contiene datos útiles para poder ser tratados por un sistema. Pueden ser datos de entrada, de proceso o de salida.

Los sistemas en los que la información que entra es distinta que la que sale, ya que ha sufrido una transformación, se denominan "sistemas de tratamiento de la información".

Diremos que el computador trabaja con información que se representa mediante códigos. Estos códigos permiten representar en función del alfabeto utilizado, todo tipo de caracteres en general. La labor de asignar un código se conoce con el nombre "codificar" y consiste en traducir un valor real para que el computador pueda interpretarlo.



T. Fernández Escudero - Elaboración propia ([CC BY](#))

Ejemplo:

La letra 'A' se representa como 00011011 utilizando el código adecuado.

El ordenador trabaja en alfabeto binario, puesto que los componentes internos solo distinguen entre dos estados. Estos dos estados los representamos como:

0 = Ausencia de información

1 = Información

A los ceros y unos los llamaremos "**bits**".

El concepto de código se define con la correspondencia que existe entre los caracteres que queramos representar y su representación.

El "código binario" será capaz de representar tantas variables como nos indique el resultado de la fórmula:

$$\text{variables} = 2^n$$

Donde n es el número de bits que tomaremos.

Autoevaluación

Mediante 8 bits podremos codificar hasta 256 valores distintos.

- Verdadero Falso

Verdadero

Sí, porque $2^8 = 256$

2.1.- Códigos Numéricos.

Recomendación

El manejo del código binario y su conversión a decimal es una destreza o habilidad imprescindible para un técnico de redes puesto que las direcciones IPv4, sus máscaras, rangos de sus subredes, sus direcciones de difusión (broadcast), etc. se calculan mediante el manejo de la conversión de decimal a binario y viceversa.

Debes conocer las propiedades del binario tan bien como conoces en decimal el multiplicar o dividir por múltiplos de 10.

Es importante también memorizar las potencias de 2 (del 0 al 8 al menos) porque se usarán constantemente.

$$2^0 = 1$$

$$2^1 = 2$$

$$2^2 = 4$$

$$2^3 = 8$$

$$2^4 = 16$$

$$2^5 = 32$$

$$2^6 = 64$$

$$2^7 = 128$$

$$2^8 = 256$$

Seguramente te resulte más sencillo comprender toda la teoría que se desarrollará a continuación visualizando algunos vídeos de Sistemas numéricos como éstos:

- 1.- [Sistemas numéricos: Binario, Decimal y Hexadecimal](#)
- 2.- [Conversión de números entre Sistemas Numéricos - Técnica RÁPIDA y FÁCIL](#)
- 3.- [\[Método Fácil\] Convertir de Binario a Decimal y viceversa.](#)
- 4.- [Como Convertir de Texto a Binario y Viceversa.](#) (Para saber cómo se manejan los caracteres en formato [ASCII](#) en formato digital/binario)

También puedes consultar la web de [CCNAdesdeCero](#) con explicaciones muy gráficas.

Las direcciones MAC y las IPv6 se representan en [hexadecimal](#). Pero es necesaria la base de binario/decimal siempre.

DECIMAL - BINARIO - OCTAL - HEXADECIMAL

Código decimal. Representa valores con los siguientes diez símbolos:

0 1 2 3 4 5 6 7 8 9

También llamado sistema en base 10, representa los números en potencias sucesivas de diez.

Ejemplo: 1972 se puede representar como:

$$1 * 10^3 = 1000$$

$$9 * 10^2 = 900$$

$$7 * 10^1 = 70$$

$$\underline{2 * 10^0} = + \underline{2}$$

1972

De esta representación podemos deducir que para representar un número como suma de potencias sucesivas de la base en la que se está, tenemos que considerar que cada dígito es un número que multiplica de derecha a izquierda a la base en la que queremos representar a dicho número de forma que esta será una potencia que empieza siendo elevada a cero y seguirá incrementando de uno en uno hasta el número más alto representado.

$$a_1 a_2 a_3 \dots a_n {}_{(10)} = 1972 {}_{(10)}$$

En Base 10 = Base₍₁₀₎

$$a_1 * 10^{n-1} + a_2 * 10^{n-2} + a_3 * 10^{n-3} + \dots + a_n * 10^{n-n}$$

$$1 * 10^3 + 9 * 10^2 + 7 * 10^1 + 2 * 10^0$$

Código binario. Representa valores con los siguientes dos símbolos:

0 1

Es un código que utiliza sólo dos dígitos {0,1}

$$a_1 * 2^{n-1} + a_2 * 2^{n-2} + a_3 * 2^{n-3} + \dots + a_n * 2^{n-n}$$

Ejemplo: 10111₍₂₎

$$1 * 2^4 + 0 * 2^3 + 1 * 2^2 + 1 * 2^1 + 1 * 2^0 = 23 {}_{(10)}$$

Código octal. Representa valores con los siguientes ocho símbolos:

0 1 2 3 4 5 6 7

Es un código que trabaja con ocho dígitos {0, 1, 2, 3, 4, 5, 6, 7}. El método más rápido para pasar a octal desde binario es hacer agrupaciones de tres dígitos del número en binario, calcular el valor decimal de cada grupo, los valores obtenidos formarán el número en octal.

$$a_1 * 8^{n-1} + a_2 * 8^{n-2} + a_3 * 8^{n-3} + \dots + a_n * 8^{n-n}$$

Ejemplo: 675₍₈₎

$$6 * 8^2 + 7 * 8^1 + 5 * 8^0 = 445 {}_{(10)}$$

Código hexadecimal. Representa valores con los siguientes dieciséis símbolos:

0 1 2 3 4 5 6 7 8 9 A B C D E F

Es un código que trabaja con diez dígitos y seis letras {0, 1, 2, 3, 4, 5, 6, 7, 8, 9, A, B, C, D, E, F}. El método más rápido para pasar de binario a hexadecimal es hacer agrupaciones de cuatro dígitos del número en binario, calcular el valor decimal de cada grupo, los valores obtenidos formarán el número en

hexadecimal. Cuando el equivalente decimal sea superior a 9, se utilizan letras, para el 10 la A, el 11 la B, el 12 la C, el 13 la D, 14 la E y el 15 la F.

$$a_1 * 16^{n-1} + a_2 * 16^{n-2} + a_3 * 16^{n-3} + \dots + a_n * 16^{n-n}$$

Ejemplo: CFA56₍₁₆₎

$$\begin{aligned} C * 16^4 + F * 16^3 + A * 16^2 + 5 * 16^1 + 6 * 16^0 &= 12 * 65536 + 15 * 4096 + 10 * 256 + 5 * 16 + 6 = 786756 + 61440 + 2560 + 80 + 6 \\ &= 850518_{(10)} \end{aligned}$$

2.2.- Equivalencia entre códigos.

La correspondencia entre los sistemas decimal, binario, octal y hexadecimal, es la representada en las siguientes tablas:

Decimal	Binario
0	0000
1	0001
2	0010
3	0011
4	0100
5	0101
6	0110
7	0111
8	1000
9	1001

Para representar diez símbolos necesitamos un mínimo de cuatro bits.

Octal	Binario
0	000
1	001
2	010
3	011
4	100
5	101
6	110
7	111

Para representar ocho símbolos necesitamos un mínimo de tres bits.

Hexadecimal	Binario
0	0000
1	0001
2	0010

3	0011
4	0100
5	0101
6	0110
7	0111
8	1000
9	1001
A	1010
B	1011
C	1100
D	1101
E	1110
F	1111

Para representar dieciséis símbolos necesitamos un mínimo de cuatro bits.

El método más rápido para pasar de un código a otro es tener el número codificado en binario y a partir de él conseguir el valor en decimal, octal o hexadecimal es una tarea sencilla.

Ejemplos:

Conversión Octal a binario:

$$56760_{(8)}$$

Si cada uno de los dígitos que forman el número octal lo tomamos como un dígito decimal y le transformamos a su equivalente binario de 3 bits, nos quedaría que:

$$5 \rightarrow 101$$

$$6 \rightarrow 110$$

$$7 \rightarrow 111$$

$$6 \rightarrow 110$$

$$0 \rightarrow 000$$

Con lo que el número en binario que se corresponde con el octal, se representa:

$$56760_{(8)} = 101\ 110\ 111\ 110\ 000_{(2)}$$

Conversión decimal a base e:

El paso de base decimal o base 10 a cualquier base se realiza dividiendo sucesivamente el número que queremos transformar utilizando como divisor la base a la que queremos pasar el número hasta que el dividendo sea menor que el divisor. El nuevo número se formará tomando como primer dígito el resultado del último cociente y los restos obtenidos en orden inverso a su obtención.

Ejemplo de conversión de decimal a binario: $23_{(10)} = 10111_{(2)}$

$$\begin{array}{r}
 23 \\
 03 \quad | \quad 2 \\
 \boxed{1} \quad | \quad 11 \quad | \quad 2 \\
 \quad \quad \boxed{1} \quad | \quad 5 \quad | \quad 2 \\
 \quad \quad \quad \boxed{1} \quad | \quad 2 \quad | \quad 2 \\
 \quad \quad \quad \quad \boxed{0} \quad | \quad 1 \\
 \hline
 10111_2
 \end{array}$$

T. Fernández Escudero - Elaboración propia ([CC BY](#))

Conversión de base n a base decimal:

El paso de cualquier base a la base diez se realiza multiplicando de derecha a izquierda los dígitos del número que estamos transformando por potencias sucesivas de la base en la que está dicho número empezando por el exponente cero. Cada resultado obtenido se suma y el resultado global es el número en base 10.

Ejemplo: Si tenemos un número en base 16:

$$CE72_{(16)}$$

Si lo expresamos en función de las potencias de 16, obtendríamos el equivalente en base decimal:

$$C*16^3 + E*16^2 + 7*16^1 + 2*16^0 = 52850_{(10)}$$

Conversión de base m a base n:

El paso correcto sería pasar de la base original a base 10 y después de base 10 a la base destino.

Ejemplo:

Si partimos de un número en base 5 y queremos realizar la conversión a base 12, primero calculamos su equivalente decimal (base 10):

$$104_{(5)}$$

$$1 * 5^2 + 0 * 5^1 + 4 * 5^0 = 29_{(10)}$$

A continuación pasamos el 29 decimal a base 12:

$$\begin{array}{r}
 29 \quad | \quad 12 \\
 \boxed{2} \quad | \quad 11 \\
 \quad \quad \quad \boxed{1} \quad | \quad 9 \\
 \quad \quad \quad \quad \boxed{0} \quad | \quad 9 \\
 \hline
 25_{(12)}
 \end{array}$$

T. Fernández Escudero - Elaboración propia ([CC BY](#))

El resultado final será: $25_{(12)}$

Autoevaluación

La dirección IP 192.168.1.1 está expresada:

2.3.- Unidades de medida.

Originalmente, se empleaban potencias de 2 al trabajar con cantidad de información y unidades de almacenamiento tipo bit y byte. Siendo $2^{10} = 1024$ y $10^3 = 1000$, los prefijos del SI se empleaban siguiendo la ley de los prefijos binarios, como se observa en las siguientes líneas.

$$k (\text{ka}) = 2^{10} = 1\,024$$

$$M (\text{Mega}) = 2^{20} = 1\,048\,576$$

$$G (\text{Giga}) = 2^{30} = 1\,073\,741\,824$$

$$T (\text{Tera}) = 2^{40} = 1\,099\,511\,627\,776$$

$$P (\text{Peta}) = 2^{50} = 1\,125\,899\,906\,842\,624$$

Sin embargo, estos prefijos mantenían y siguen manteniendo el significado de las potencias de 1000 cuando de lo que se trata es de expresar la velocidad de la transmisión de datos (cantidad de bits): por ejemplo una red Ethernet de 10 Mbit/s es capaz de transmitir 10 000 000 bit/s, y no 10 485 760 bit/s. El problema se acrecienta por no ser las unidades de información bit y byte unidades del SI. En el SI el bit, el byte, el baudio o la cantidad de signos se darían en hercios. Aunque es más claro emplear "bit" para el bit y "b" para el byte, a menudo se emplea "b" para el bit y "B" para el byte (en el SI, B es la unidad del belio, siendo la del decibelio dB).

Por toda esta confusión, en el año 1998, la Comisión Electrotécnica Internacional (International Electrotechnical Commission —IEC—), eligió nuevos prefijos binarios, que consisten en colocar un 'bi' tras la primera sílaba del prefijo decimal (siendo el símbolo binario como el decimal más una 'i'). Por lo tanto, ahora un kilobyte (1 kB) son 1000 byte, y un kibibyte=(1 KiB)= 2^{10} bytes = 1024 octetos o bytes. De la misma forma, un mebibyte= MiB= 2^{20} bytes, un gibibyte= 1 GiB= 2^{30} bytes, tebi (Ti; 2^{40}), pebi (Pi; 2^{50}) y exbi (Ei; 2^{60}). Aunque el estándar del IEC nada diga al respecto, los siguientes prefijos alcanzarían hasta zebi (Zi; 2^{70}) y yobi (Yi; 2^{80}).

Hasta el momento el empleo de esta última notación (KiB) ha sido muy escasa y en muchas ocasiones se siguen usando potencias de 2 para los kB.

Debes conocer

Hay que prestar mucha atención al tema de los bits, los Bytes (8 bits) y los "Megas", "Gigas", etc.

Por ejemplo, la forma correcta de expresar una **cantidad de información (almacenada)** de un Mega, sería en Bytes (**MB**), mientras que en **transmisión de información** se expresa como una velocidad de bits por segundo (**Mbps** ó **Mb/s**). Fíjate en la **B mayúscula para Bytes y b minúscula para bits**.

Ejercicio Resuelto

Calcula los siguientes tiempos, suponiendo que tenemos en una LAN un PC conectado mediante GigaEthernet a un router que tiene una conexión WAN de fibra de "400 Megas". En todos los casos se deben dejar todas las cuentas indicadas, expresadas las multiplicaciones, divisiones y/o potencias, y además calcular el resultado).

a) ¿Cuánto tiempo se tardaría como mínimo en descargar desde el PC un fichero de 500000 Kas?

b) Si después de descargar ese fichero en el PC, queremos copiarlo a otro PC de su misma LAN ¿cuánto tardaría en copiarlo como mínimo si el 2º PC está conectado por...

b.1) GigaEthernet?

b.2) WiFi 802.11n sin encriptación, 1 sola antena MIMO y cobertura máxima?

Mostrar retroalimentación

Descargar 500000 Kas con 400 Megas

Tiempo = Cantidad de Info / Velocidad de Descarga = $5 * 10^5 * 10^3 * 8 \text{ bits} / (400 * 10^6) \text{ bits/s} =$

10 segundos

Con potencias de 2 (antes de 1998)

Tiempo = Cantidad de Info / Velocidad de Descarga = $5 * 10^5 * 2^{10} * 8 \text{ bits} / (400 * 10^6) \text{ bits/s} =$

10,24 segundos

Con GigaEthernet:

Tiempo = Cantidad de Info / Velocidad de Descarga = $5 * 10^5 * 10^3 * 8 \text{ bits} / (10^9) \text{ bits/s} =$

4 segundos

Con 802.1n https://en.wikipedia.org/wiki/IEEE_802.11n-2009#Data_rates

Con un solo stream (1 antena) y 40MHz se puede alcanzar como máximo 150Mb/s

Tiempo = Cantidad de Info / Velocidad de Descarga = $5 * 10^5 * 10^3 * 8 \text{ bits} / (150 * 10^6) \text{ bits/s} =$

26,66666667 segundos

3.- Arquitecturas de redes. Conceptos básicos.

Caso práctico

Una de las principales tareas a la hora de configurar una red local es la de establecer la mejor arquitectura de red en función de los servicios que va a proporcionar y los protocolos con los que van a trabajar. Esto es lo que **Laro** explica a **Jana**, que estuvo realizando en una práctica el pasado curso mientras estaba en su misma situación, realizando el módulo de FCT.

Ella comenta que recuerda que lo vieron en clase y que había una serie de conceptos importantes que tuvo que aprender, pero que ahora, al llevarlos a la práctica, es cuando los entiende realmente.



Alain Bachellier (CC BY-NC-SA)

Debes conocer

En adelante se profundizará en el estudio de 2 **arquitecturas de red** principales:

- 1.- La arquitectura **OSI** (de 7 capas) que es una base más bien **teórica** cuya implantación real no ha tenido gran repercusión salvo en contados protocolos, pero su **nomenclatura** sí que se usa extensivamente.
- 2.- La arquitectura **TCP/IP** (de 4 capas) que fue una implementación "real" y temprana que se impuso desde el principio y hasta el día de hoy, aunque coloquialmente **se mezclan** conceptos y nomenclatura con la OSI.

Las arquitecturas de redes vienen definidas por tres características fundamentales:

Protocolos de alto nivel: Nos dicen cómo se comunican las aplicaciones.

Protocolos de bajo nivel: Definen cómo se transmiten las señales a nivel físico, por ejemplo por el cable.

Protocolos de nivel medio: Son protocolos más difíciles de explicar porque rigen el funcionamiento de los niveles intermedios, que son los niveles menos visibles. Un ejemplo serían los protocolos de acceso al medio (**CSMA/CD**).

El diseño de una red de comunicaciones, evidentemente, es bastante complejo. Algunos de los problemas más importantes a los que se enfrentan los diseñadores de estas redes son:

Direccionamiento.- Una red normalmente tiene muchos ordenadores conectados, algunos de los cuales tienen múltiples procesos (programas), por lo tanto necesitamos de un mecanismo para que un proceso en una máquina especifique con quién quiere comunicarse en el otro extremo. Dicho de otro modo, los datos que se envían deben contener suficiente información de identificación para llegar al destino correcto.

Encaminamiento.- Una vez que tengamos diseñado los mecanismos que nos permitan identificar los procesos en las distintas máquinas de una red (direccionamiento), y en el caso en que en esa red haya distintos caminos, debemos de enfrentarnos al problema de elegir la mejor ruta a seguir; normalmente será la más corta o la que en ese momento tenga menor tráfico.

Acceso al medio.- En las redes donde existe un medio de comunicación compartido, debe de haber algún mecanismo que controle el orden de transmisión de los interlocutores. De no ser así, todas las transmisiones se interfieren y no será posible llevar a cabo una comunicación en óptimas condiciones. El control de acceso al medio en una red es muy similar a una comunicación mediante walkie-talkie, donde los dos interlocutores deben evitar hablar a la vez o se producirá una colisión.

Problema de saturación del receptor.- Consiste en que un emisor rápido pueda saturar a un receptor lento. En determinadas condiciones el proceso en el otro extremo necesita un tiempo para procesar la información que le llega. Si ese tiempo es demasiado grande en comparación con la velocidad con la que le llega la información, será posible que se pierdan datos. Una posible solución a este problema consiste en que el receptor envíe un mensaje al emisor indicándole que está listo para recibir más datos.

Mantenimiento del orden.- Algunas redes de transmisión de datos desordenan los mensajes que envían, de forma que, si los mensajes se envían en una secuencia determinada, no se asegura que lleguen en esa misma secuencia. Para solucionar esto, el protocolo debe incorporar un mecanismo que le permita volver a ordenar los mensajes en el destino. Este mecanismo puede ser la numeración de los fragmentos, por ejemplo.

El control de errores.- Todas las redes de comunicación de datos transmiten la información con una pequeña tasa de error, que en ningún caso es nula. Esto se debe a que los medios de

transmisión son imperfectos. Tanto emisor como receptor deben ponerse de acuerdo a la hora de establecer qué mecanismos se van a utilizar para detectar y corregir errores, y si se va a notificar al emisor que los mensajes llegan correctamente.

El problema de compartir un canal.- En determinadas ocasiones, la red puede tener tramos en los que existe un único medio de transmisión que, por cuestiones económicas, debe ser compartido por diferentes comunicaciones que no tienen relación entre sí, es lo que se conoce como multiplexación. Así, el protocolo deberá asegurar que todas las comunicaciones que comparten el mismo medio no se interfieran entre sí.

Por último señalar que, para que la comunicación entre dos equipos en una red sea efectiva, a los datos que se transmiten habrá que añadirles una información "extra" en cada capa o nivel en función del protocolo usado, esta información ayudará en ese proceso de comunicación y a todo este proceso entre capas y protocolos se llama **encapsulamiento**.

Recomendación

Visualiza el siguiente [vídeo dónde resume y compara las 2 arquitecturas de red](#) que veremos en la unidad y explica con ejemplos el concepto de **Encapsulamiento entre capas**.

Autoevaluación

El proceso de encapsulamiento consiste en meter un equipo de red en una cápsula plástica.

- Verdadero Falso

Falso

3.1.- Capa (o nivel), Servicio, Interfaz y Protocolo.

Las redes se organizan en **capas o niveles** para reducir la complejidad de su diseño ("divide y vencerás"). Cada nivel es responsable de ofrecer servicios a niveles superiores. A la arquitectura por niveles también se la llama **Jerarquía de Protocolos**.

Cuando se diseña una determinada arquitectura se deben cumplir entre otras, las siguientes reglas:

Cada nivel dispone de un conjunto de servicios.

Los servicios están definidos mediante protocolos estándares.

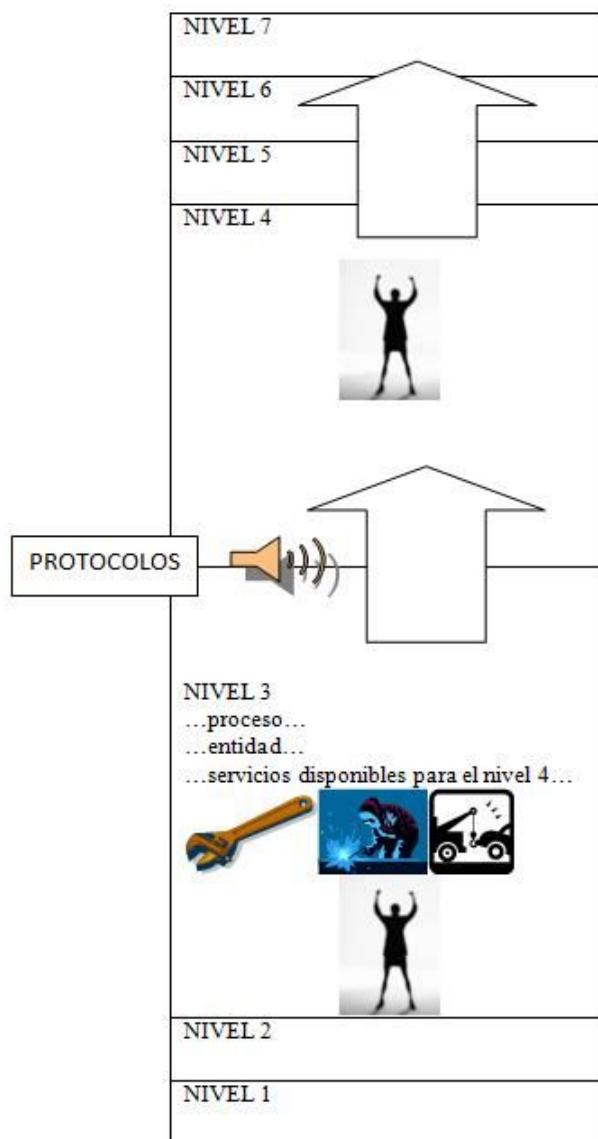
Cada nivel se comunica solamente con el nivel inmediatamente superior y el inmediatamente inferior.

Los niveles inferiores proporcionan servicios a los niveles superiores.

Los niveles de dos equipos diferentes se tienen que poner de acuerdo y utilizar las mismas reglas de transmisión (mismo protocolo).

A los elementos activos de cada capa se les llama entidades o procesos y son estos los que se comunican mediante el uso del protocolo.

A las entidades o procesos en máquinas diferentes que están al mismo nivel se les llama entidades pares o procesos pares.



"Los servicios utilizan los protocolos para que haya comunicación entre los niveles"

3.1.1.- Servicios.

Los servicios se pueden clasificar en:

- Orientados a la conexión.
- No orientados a la conexión.
- Confirmados (fiables).
- No confirmados (no fiables).

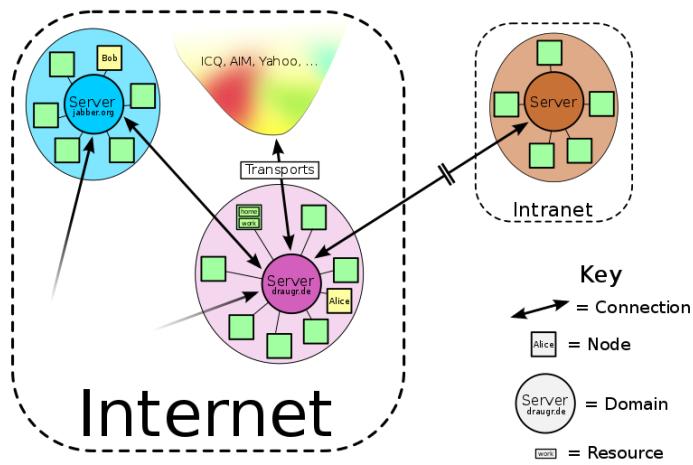
Los servicios posibles de una capa son:

- Servicios orientados a la conexión y confirmados.
- Servicios orientados a la conexión y no confirmados.
- Servicios no orientados a la conexión y confirmados.
- Servicios no orientados a la conexión y no confirmados.

Los servicios básicos son:

- CONNECT**: Para establecer una conexión. Se utiliza en comunicaciones orientadas a la conexión.
- DISCONNECT**: Se utiliza para liberar una conexión y terminar la conexión. Servicio orientado a la conexión.
- DATA**: Para enviar información, tanto orientado a la conexión como sin conexión.

Cuando una capa cualquiera de la arquitectura desea establecer una conexión con su homónima remota, deberá realizar una llamada al servicio **CONNECT** de la capa que tienen debajo. Ésta, a su vez, también debe realizar esa llamada, a no ser que se trate de la capa más inferior. Lo mismo ocurre con los servicios **DISCONNECT** y **DATA**.



XZise (CC BY-SA-3.0)

3.1.2.- Primitivas.

Un servicio está definido por un conjunto de operaciones más sencillas llamadas primitivas.

Primitiva	Significado
Request (petición)	Solicitud para realizar una acción
Indication (indicación)	Notificación de que ha ocurrido un suceso
Response (respuesta)	Solicitud de respuesta a un suceso
Confirm (confirmación)	Notificación de que ha llegado la respuesta de una acción anterior

Las primitivas no "viajan" entre las estaciones que se comunican. Los mensajes de control o de datos se envían como consecuencia de una llamada a la primitiva correspondiente.

Las primitivas tampoco son recibidas, sino que son utilizadas para notificar a la capa que el mensaje ha sido recibido y está disponible para su inspección o tratamiento. Por lo tanto, las primitivas de solicitud de envío funcionan como "llamadas al sistema", están en cada capa y se activan dependiendo de la tarea a realizar.

Servicio.Primitiva	Parámetros
CONNECT.request	Dirección de la estación de destino. Servicio requerido. Tamaño máximo del mensaje.
CONNECT.indication	Dirección de la estación de origen. Servicio que solicita. Tamaño máximo del mensaje.
CONNECT.response	Aceptación de la conexión. Tamaño máximo del mensaje.
CONNECT.confirm	Aceptación de la conexión. Tamaño máximo del mensaje.
DATA.request	Dirección destino. Mensaje a enviar. Tamaño del mensaje. Número de mensaje (para el orden).
DATA.indication	Dirección de origen. Mensaje recibido. Tamaño del mensaje. Número del mensaje.
DATA.response	Número de mensaje recibido. ¿Hay error?
DATA.confirm	Número de mensaje recibido. ¿Hay error?
DISCONNECT.request	

Reglas básicas a la hora de trabajar con primitivas:

El servicio CONNECT siempre es confirmado, por lo que, si aparece, llevará siempre las primitivas request, indication, response y confirm.

Impide la pérdida accidental de datos.

Opción al otro extremo de poder negar determinadas solicitudes de conexión.

Permite que ambos interlocutores puedan negociar las condiciones de la comunicación.

El servicio DATA puede ser confirmado o no. Si es no confirmado, sólo llevará las primitivas request e indication.

El servicio DISCONNECT suele ser no confirmado, aunque a veces hay que asegurar que los dos extremos finalizan la comunicación y así liberan sus recursos reservados.

El siguiente gráfico representa una comunicación entre dos niveles reflejando los servicios y las primitivas que intervienen.

T. Fernández Escudero - Elaboración propia ([CC BY-SA](#))

Autoevaluación

¿Cuál es la diferencia entre servicios y protocolos?

- No hay ninguna diferencia.
- Los servicios se sirven de los protocolos.
- Los protocolos utilizan los servicios.
- Los protocolos son los interfaces y los servicios las capas.

No es correcto. Parece que no has entendido estos conceptos.

Correcto. Los servicios utilizan los protocolos para comunicar las capas a través de las interfaces.

No es correcto. Creo que debes volver a leer el apartado.

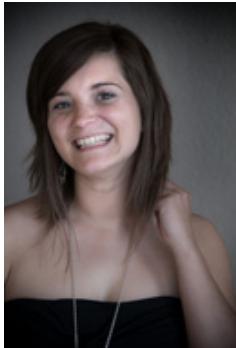
No es correcto. Deberías repasar el tema.

Solución

1. Incorrecto
2. Opción correcta
3. Incorrecto
4. Incorrecto

4.- Encapsulamiento de la Información. Características de las arquitecturas por niveles o capas.

Caso práctico



Jana ya sabe lo que son los protocolos y qué protocolo utiliza su ordenador para ser identificado en la red. Y como primera práctica ha utilizado el comando ping para verificar la conexión entre dos ordenadores, pero le ha surgido una duda, entre los mensajes que se producen como resultado de esta orden hay uno que dice "paquetes enviados...", ha buscado en Internet información y lejos de aclararse, se ha liado más porque los documentos que ha encontrado hablan de "datos, tramas, paquetes...".

Cree que lo mejor será preguntar a alguien de la empresa, aunque teme quedar como una tonta.

[Alain Bachellier \(CC BY-NC-SA\)](#)

Cuando se comunican dos ordenadores que utilizan la misma arquitectura de red, los protocolos que se encuentran al mismo nivel deben coordinar el proceso de comunicación. El motivo final de la comunicación será la transmisión de los datos generados en la capa de aplicación, pero para ello los datos deben de ir bajando por las distintas capas, y estas les irán agregando una información, de forma que sea comprensible para la capa de su mismo nivel en el ordenador de destino. Por ejemplo, el nivel 2 de un equipo (transmitiendo) coordina sus actividades con el nivel 2 del otro extremo (que se encargaría de recibir). Esto quiere decir que ambos deben ponerse de acuerdo y utilizar las mismas reglas de transmisión (es decir, el mismo **protocolo**).

A los elementos activos de cada capa se les llama entidades o procesos y son éstos los que se comunican mediante el uso del **protocolo**. Al grupo formado por las entidades o procesos en máquinas diferentes que están al mismo nivel se llaman entidades pares o procesos pares.

El modelo de arquitectura por niveles necesita información adicional para que los procesos pares puedan comunicarse a un determinado nivel.

A estos datos adicionales, añadidos en cada capa, se les llama **cabecera o información de control** y suele ir al principio del mensaje. Comúnmente este proceso se denomina **encapsulado de datos o encapsulación**.

La forma que adopta la información en cada capa se denomina PDU (Unidad de datos del protocolo). Durante la encapsulación, cada capa encapsula las PDU que recibe de la capa superior añadiéndole la correspondiente cabecera. En el receptor, a su llegada, estas unidades de datos sufren el proceso contrario de **desencapsulado**. Conforme la PDU va pasando de una capa a la capa inmediatamente superior, se le va quitando la información de control que puso el emisor.

En cada etapa del proceso, una PDU tiene un nombre distinto para reflejar su nuevo aspecto. Aunque no existe una convención universal de nombres para las PDU, en este curso las vamos a denominar de acuerdo con los protocolos de la arquitectura TCP/IP:

Datos: el término general para las PDU que se utilizan en la capa de aplicación.

Segmento: PDU de la capa de transporte.

Paquete: PDU de la capa de red.

Trama: PDU de la capa de enlace.

Bits: PDU que se utiliza cuando se transmiten físicamente datos a través de un medio.

Se muestra a continuación un diagrama simplificado del proceso de encapsulación en TCP/IP de un mensaje proveniente de la capa de aplicación hasta llegar al nivel de trama con los diferentes "direcciónamientos" en cada capa (puertos en TCP/UDP, direcciones IP y direcciones MAC):

Alfonso Bonillo - elaboración propia . Proceso de encapsulamiento (Dominio público)

El crecimiento tan rápido sufrido por las redes locales, que hoy en día se han expandido hasta formar la red Internet, ha impedido la consolidación de un estándar global que definiera el punto de partida sobre las especificaciones y protocolos de transmisión de datos.

Se han realizado esfuerzos considerables para obtener un estándar común para todas las redes de los diferentes fabricantes (como es el modelo OSI), pero se ha comprobado que esos esfuerzos que se han realizado han llegado demasiado tarde y **en la práctica** se usa el modelo TCP/IP mezclado con algunas nomenclaturas del modelo OSI.

En los siguientes apartados se verán los modelos más utilizados actualmente para redes de ordenadores.

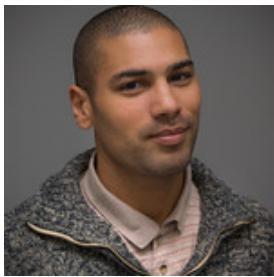
Autoevaluación

Trama es un concepto que se refiere a:

5.- El Modelo OSI y sus capas o niveles.

Caso práctico

Visto que hay diferentes formas de llamar a los datos que circulan por la red dependiendo del nivel o capa que se esté considerando, la duda que **Naroba** le plantea a **Vindio** es que no termina de entender las diferencias entre los modelos OSI y TCP/IP. ¿Qué diferencias hay en cada capa? ¿Por qué no unifican un solo modelo?



[Alain Bachellier \(CC BY-NC-SA\)](#)

Vindio entiende su pregunta y comparte el que debería ser unificado un solo modelo, especialmente para no liar a los estudiantes. Pero le explica que cada uno tiene su razón de ser y que las diferencias entre ambos surgen por el modo de entender el recorrido que hacen los datos al ser enviados desde un emisor a un receptor, así que podemos decir que ambos modelos tienen en común el que hay quien envía datos y quien los recibe. Y ambos modelos tienen niveles mayor y menor



[Alain Bachellier \(CC BY-NC-SA\)](#)

El modelo OSI de ISO es un modelo que se creó para poder estandarizar todos los protocolos, contempla siete niveles de estudio en la arquitectura de red. Los siete niveles son los que aparecen en el diagrama de la izquierda.

Si queremos que dos equipos establezcan una comunicación entre ellos, estos equipos deben hablar el mismo lenguaje y además se deben de poner previamente de acuerdo en una serie de normas. Estas normas, son los denominados protocolos.

El problema que apareció en un primer momento, era que cada fabricante diseñaba protocolos diferentes. De esta forma, nos encontrábamos con redes imposibles de interconectar. Evidentemente, era necesario crear un diseño que sirviera como estándar, de ahí surge el modelo de referencia OSI.

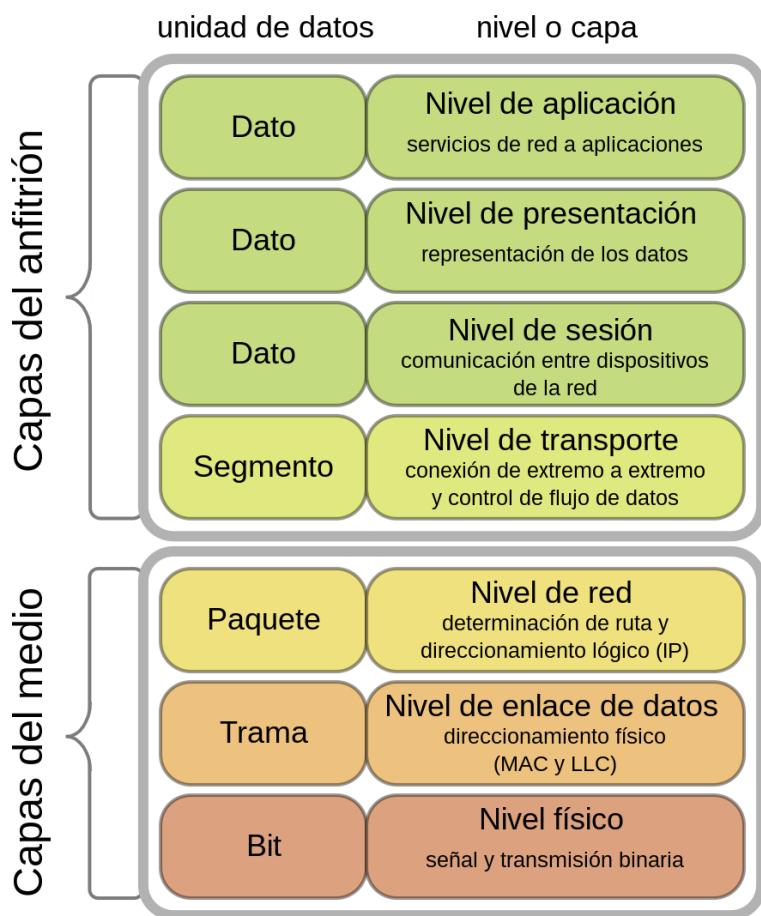
El modelo OSI (Open Systems Interconnection o Interconexión de Sistemas Abiertos) está basado en una propuesta establecida en el año 1983 por la organización internacional de normas ISO como un avance hacia la normalización a nivel mundial de protocolos. El modelo se llama modelo de referencia OSI de la ISO, puesto que se ocupa de la conexión de sistemas abiertos, esto es, sistemas que están preparados para la comunicación con otros sistemas diferentes.

OSI no prosperó como TCP/IP porque cuando se quiso implantar, los protocolos TCP/IP ya eran empleados por la mayoría de los centros de investigación.

OSI es una división más académica que técnica y algunas de las capas que contempla, casi no tienen sentido porque apenas se diferencian entre sí (Sesión, Presentación, Aplicación).

El modelo OSI fue un modelo que se creó sobre la teoría y luego se intentó llevar a la práctica. Es, desde el punto de vista académico, muy bueno para estudiar la arquitectura de las redes, aunque menos práctico que el TCP/IP.

Como ya hemos visto, el diseño de un sistema de comunicación requiere de la resolución de muchos y complejos problemas. Por este motivo, y para reducir la complejidad de este diseño, las redes se organizan en capas o niveles. De esa manera, la comunicación entre ordenadores queda estructurada por niveles y forma lo que llamaremos una arquitectura de protocolos de comunicaciones.



[Offnfopt. Capas del modelo OSI y sus PDUs](#) (Dominio público)

únicamente al inmediatamente superior

A continuación veremos las funciones encomendadas a cada una de las capas de OSI:

1.- Nivel físico: es la capa de más bajo nivel y se encarga de la transmisión de dígitos binarios por un canal de comunicación. Esta capa define las especificaciones desde distintos puntos de vista, lo vemos con algunos ejemplos:

Mecánico: el tipo de cable (coaxial, par trenzado, fibra óptica), el medio inalámbrico que utilizamos, ...

Eléctrico: ¿qué voltaje deberá usarse para representar un 1 o un 0?, ¿cuántos microsegundos dura cada digito?, ¿en qué frecuencia de radio se va a transmitir?, ...

Funcionales: ¿cuántas puntas tiene el conector de la red y para qué sirve cada una de ellas?, tipo de conectores, ...

La capa física, en última instancia, será la encargada de pasar a señal eléctrica, lumínica o de radio, los datos que reciba en formato digital.

2.- Nivel de enlace de datos: su tarea principal es detectar y corregir todos los errores que se produzcan en la línea de comunicación. También se encarga de controlar que un emisor rápido no saturé a un receptor lento, ni que se pierdan datos innecesariamente.

En redes donde existe un único medio compartido por el que circula la información, este nivel se encarga también de repartir su utilización entre las estaciones.

La unidad mínima de datos que se transfiere entre entidades pares en este nivel se llama trama, siendo los protocolos de esta capa los responsables de delimitar el comienzo y el final de cada trama, escribiendo para ello ciertos códigos al comienzo y al final de la misma.

3.- Nivel de red: se ocupa de determinar cuál es el mejor camino para enviar información entre el origen y el destino, pudiendo pasar por tantas redes intermedias como sea necesario. Es en este nivel de red donde los datos se fragmentan en paquetes, enviándose cada uno de ellos de forma independiente. Estos paquetes irán por el camino más adecuado de forma que lleguen en el menor tiempo posible.

OSI emplea esta arquitectura en niveles a fin de dividir los problemas de interconexión en partes manejables. También esta aproximación en niveles facilita que el software pueda mejorarse sin necesidad de introducir cambios revolucionarios, permitiendo además la compatibilidad entre equipos diferentes. OSI consta de siete capas o niveles, mostrados en la tabla siguiente, y que son: físico, enlace, red, transporte, sesión, presentación y aplicación.

En una arquitectura diseñada en capas o niveles, debemos de tener siempre presente los siguientes aspectos:

Cada capa de la arquitectura está pensada para realizar una función bien definida.

Cada nivel debe interaccionar únicamente con los niveles contiguos a él, es decir, el superior y el inferior.

Cada nivel se sirve del inmediatamente inferior para que realice una tarea para él.

Cada nivel presta servicio

(camino más corto, el más rápido, el que tenga menor tráfico, etc). Esta capa debe controlar también la congestión de la red, intentando repartir la carga lo más equilibrada posible entre las distintas rutas. La unidad mínima de información que se transfiere a este nivel se llama paquete o datagrama.

4.- Nivel de transporte: permite asegurar que los datos lleguen correctamente de un extremo a otro de la comunicación al nivel de sesión. Para ello establece mecanismos fiables para el intercambio de datos, realizando servicios de detección de errores. Además el nivel de transporte será el encargado de recomponer la información, eliminando las tramas repetidas y colocándolas en el orden correcto.

5.- Nivel de sesión: proporciona servicios para que aplicaciones muy específicas puedan dialogar entre sí, para ello se crean conexiones denominadas sesiones. Establece mecanismos para la reanudación de la comunicación después de un error fatal (fallo en la red, una interrupción, etc), determinando el punto exacto sobre el que reanudar el diálogo entre dispositivos.

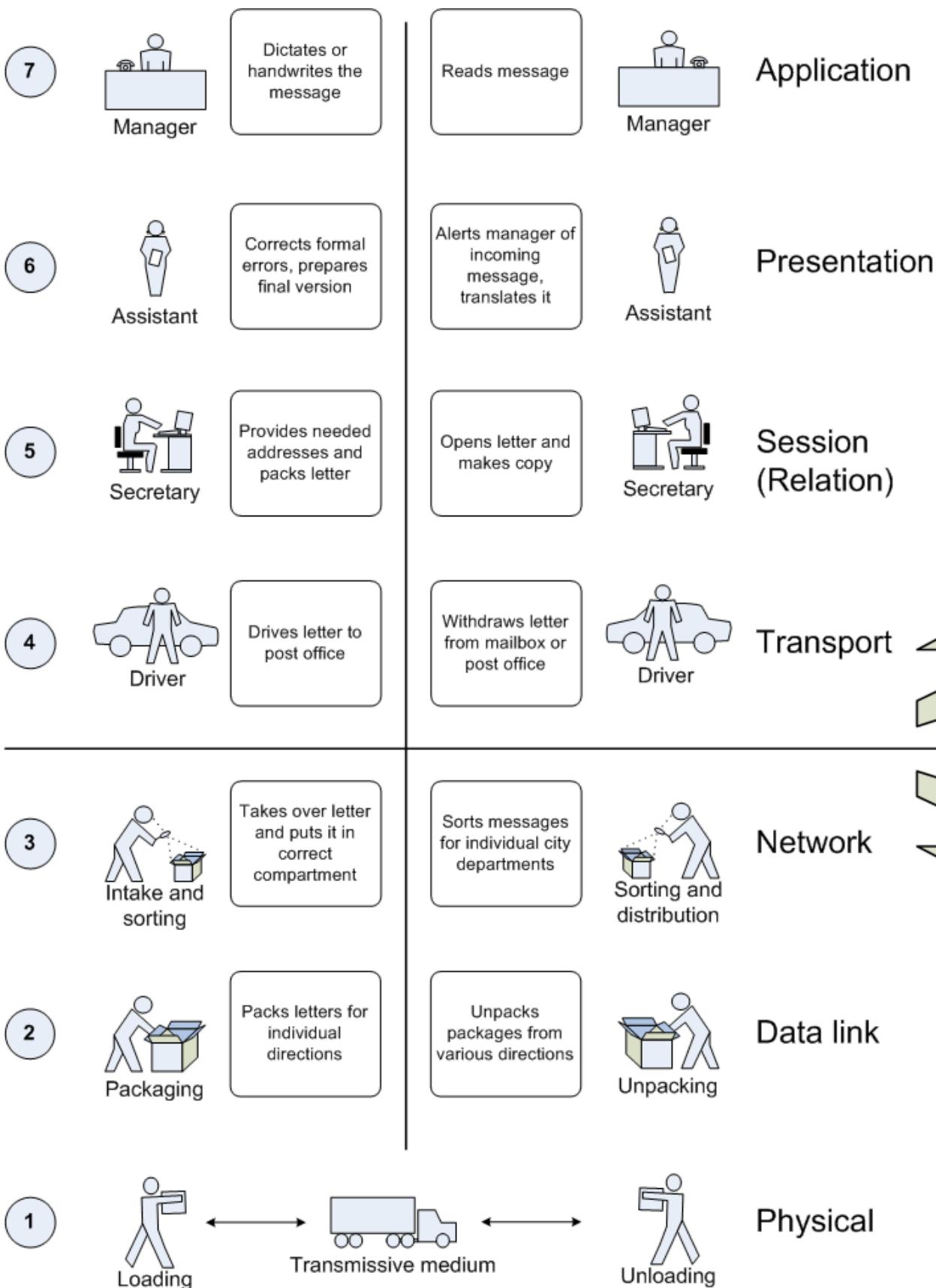
6.- Nivel de presentación: estará encargado de la presentación de los datos, actuando como un traductor entre las estaciones. Por ejemplo, si una estación trabaja con un código concreto y la estación del otro extremo maneja uno diferente, el nivel de presentación es el responsable de realizar esta conversión. Para conversaciones confidenciales, este nivel también codifica y encripta los datos para hacerlos incomprensibles a posibles escuchas ilegales.

7.- Nivel de aplicación: es el nivel que está en contacto directo con los programas o aplicaciones informáticas de las estaciones y contiene los servicios de comunicación más utilizados en las redes. Como ejemplos de servicios a este nivel se puede mencionar la transferencia de archivos, el correo electrónico, etc.

Por último, conviene aclarar, que el modelo de referencia OSI está definido como un modelo teórico que no se aplica realmente a la práctica, ya que ISO definió solamente la función general que debe realizar cada capa, pero no mencionó en absoluto los servicios y protocolos que se deben usar en cada una de ellas. Además cuando apareció OSI ya otros modelos se habían implantado de forma generalizada a causa de Internet, como es la pila de protocolos TCP/IP. No obstante, en el estudio y el diseño de las redes, el modelo de referencia OSI juega un papel importante para conocer y entender mejor su funcionamiento.

El siguiente diagrama establece un paralelismo en cómo se organiza el envío de cartas por correos entre 2 empresas con el modelo OSI. En algunos casos se puede ver el paralelismo realmente y otras no encaja del todo, pero cuando menos es interesante la imagen y puede ayudar a comprender el concepto de encapsulamiento como meter información dentro de sobres, sobres dentro de cajas, cajas dentro de camiones, etc.

Company's business



RM – OSI and letter communication parallel

Para saber más

En el siguiente videotutorial se explica algunas características del modelo de referencia OSI: [Modelo de referencia OSI](#)

Puedes ver otro paralelismo y más explicaciones en el [curso de Aulaclic](#).

5.1.- Físico.

El nivel Físico se encarga de estudiar todo lo relativo al medio de transmisión físico, características técnicas, eléctricas, mecánicas y de composición. En este nivel se definen los estándares que especifican por ejemplo, el tipo de medio físico (cable de cobre, fibra óptica o medio inalámbrico) que se va a utilizar para conectar los diferentes dispositivos de una determinada red, pero también la codificación de las señales de los dígitos binarios que forman las tramas de la capa anterior.

[Blair Bonnett \(CC BY-SA-4.0\)](#)

Página 25 de 83

5.1.1.- Especificaciones.

Como hemos comentado antes, el nivel físico se encarga de las conexiones físicas de la red, tanto en lo que se refiere al medio físico como a la forma en la que se transmite la información. Y su funcionalidad se centra en los siguientes puntos:

Características mecánicas y eléctricas.

Métodos de transmisión de dígitos binarios por un canal de comunicación.

Mecanismos que verifiquen que, cuando un lado envíe un "1", se recibe en el otro lado como "1" y no como "0".

Voltaje que deberá usarse para representar un 1 y un 0.

Microsegundos que dura un dígito.

Frecuencia de emisión.

Puntas que tiene el conector de red y para qué sirve cada una.

[EU General Federation \(CC BY-SA\)](#)

Autoevaluación

El nivel físico se encarga de que el voltaje y la frecuencia sean correctas en una conexión.

- Verdadero Falso

Verdadero

5.1.2.- Objetos de estudio en el Nivel Físico.

Conocer el nivel Físico del modelo OSI implica entender muchos conceptos básicos de sistemas electrónicos y digitales, entre los que destacamos:

Medios de transmisión de señal:

Cables de pares

Cables coaxiales

Fibra óptica

Transmisión vía satélite

Transmisiones y distintas técnicas de modulación.

Técnicas de multiplexación.

Técnicas de concentración de canales.

Técnicas de conmutación:

De circuitos.

De mensajes.

De paquetes.

Transmisión en serie o en paralelo.

Transmisión síncrona o asíncrona.

Normas de conexión en el nivel físico.

[Ian Andrei \(CC BY-SA\)](#)

Para saber más

La capa física controla la manera en que se transmiten los datos en el medio de comunicación. En el siguiente enlace encontrarás el capítulo del curso Aspectos básicos de networking de CCNA Exploration dedicado al Nivel Físico del modelo OSI.

[Nivel Físico del Modelo OSI](#)

5.1.3.- Funciones del Nivel Físico.

Vamos a ver las funciones generales de la capa física, con que los estándares y protocolos que administran la transmisión de datos a través de medios locales. Todo eso se resume en los siguientes puntos:

- Definir el medio o medios físicos por los que va a viajar la comunicación: cable de pares trenzados, coaxial, guías de onda, aire, fibra óptica.
- Definir las características materiales (componentes y conectores mecánicos) y eléctricas (niveles de tensión) que se van a usar en la transmisión de los datos por los medios físicos.
- Definir las características funcionales de la interfaz (establecimiento, mantenimiento y liberación del enlace físico).
- Transmitir el flujo de bits a través del medio.
- Manejar las señales eléctricas/electromagnéticas.
- Especificar cables, conectores y componentes de interfaz con el medio de transmisión.
- Garantizar la conexión (aunque no la fiabilidad de ésta).

[CristianZambrano \(CC BY-SA-3.0\)](#)

Para saber más

Recomendamos la descarga de la siguiente presentación sobre las señales de comunicación en el nivel físico del modelo OSI.

[La Capa Física señales de Comunicación.pptx](#)

5.2.- Enlace.

Se encarga de describir cómo los niveles superiores utilizan el medio físico para transmitir o recibir información, es el más complicado de comprender puesto que tiene difícil acceso para el usuario. Se estudian protocolos de "acceso al medio" como pueden ser el CSMA/CD (acceso múltiple por examen de portadora con detección de colisiones).

[Frealsanchez \(CC BY-SA-3.0\)](#)

Autoevaluación

Si solo está un equipo transmitiendo en un mismo tiempo es imposible que se produzca una colisión.

- Verdadero Falso

Verdadero

5.2.1.- Funciones.

Para conseguir que la comunicación de datos a través de un medio físico se produzca correctamente, se necesita controlar el intercambio de datos. Este control se lleva a cabo por una capa que se coloca por encima del nivel físico y que se denomina nivel de enlace.

El nivel enlace se encarga de controlar los datos del nivel físico y además proporcionar datos fiables al nivel inmediatamente superior (nivel red).

Para que los datos se transmitan correctamente por el enlace, además de un medio físico adecuado son necesarios:

Sincronización a nivel de trama.

Control de flujo: La estación emisora y al receptora deben ponerse de acuerdo en el ritmo de transmisión de datos.

Control de errores.

Direccionamiento: Si existe más de un posible destino de un mensaje es necesario identificarlo perfectamente.

El nivel enlace se encarga de la creación y el envío de tramas. En la capa física el envío de información se hace en forma de bits; la capa de enlace actúa de manera distinta, construye con los bits paquetes discretos denominados tramas (frames) que son los que envían por la línea. Según el tipo de red la trama puede variar en tamaño. La utilización de las tramas permite simplificar el proceso de detección de errores así como mejorar la capacidad de transmisión del medio mejorando el que sea compartido.

[Anónimo \(CC BY\)](#)

5.2.2.- Control de Flujo.

Otro mecanismo de este nivel es el control de flujo, una técnica que posibilita que el emisor no sature con demasiada información al receptor. El receptor establece una zona de almacenamiento temporal donde va acumulando la información que recibe. El receptor utiliza esta zona para manipular la información y proporcionar los datos correctos al nivel de red (control de errores y ordenación de tramas).

Si no existiese el control de flujo, esta memoria se podría desbordar y se podría llegar a perder información creando colapsos en la red.

[Isometrik \(CC BY-SA-3.0\)](#)

5.2.3.- Detección y corrección de errores.

En este nivel es donde aparece por primera vez un intento de verificar que la información se transmita correctamente. Se trata de implantar sistemas de detección y/o corrección de errores a nivel binario. Los métodos más utilizados para ello son:

- Usar bits de paridad.
- La suma de verificación.
- El código de redundancia cíclica (CRC).

Alfonso Bonillo - Elab.Propia (Dominio público)

Alfonso Bonillo - Elab.Propia (Dominio público)

Alfonso Bonillo - Elab.Propia (Dominio público)

Para saber más

En el siguiente enlace puedes conocer más cosas sobre estos tres sistemas de verificación.

[Detectar y corregir errores en la capa de enlace.](#)

Autoevaluación

¿Los bits de paridad, el CRC y el Checksum sirven para detectar errores en la transmisión?

- Verdadero Falso

Verdadero

5.2.4.- Mecanismos de control del canal.

Las redes locales suelen utilizar la tecnología de difusión (broadcast); en las redes de difusión el canal es compartido por todos los ordenadores de la red. Normalmente, cada mensaje transmitido tiene un único destinatario, cuya dirección aparece en el mensaje, pero para saber si el mensaje es para él, cada ordenador de la red ha de escuchar cada mensaje, analizar la dirección de destino y comprobar si coincide con la propia, descartándolo en caso contrario. Por esta razón, se debe tener un mecanismo que permita a cada ordenador utilizar el canal durante un determinado tiempo para poder enviar la trama a la red. Los protocolos deberán proporcionar los medios para que no haya pérdida de datos ni conflictos.

Debido al problema del reparto del canal en el acceso al medio, en las redes de difusión, la capa de enlace adquiere una configuración más compleja que en las redes punto a punto. Esta es la razón por la cual, para su estudio e implementación, se la suele dividir en dos subcapas:

MAC: Control de Acceso al Medio (Media Access Control). Controla el acceso al medio de transmisión.

LLC: Control de Enlace Lógico (Logical Link Control), más superficial que la MAC.

Los protocolos diseñados para gobernar el reparto de canal tienen su origen en los protocolos aloha simple y aloha ranurado .

En 1970, un equipo de la Universidad de Hawái (Norman Abramson) quería conectar terminales de ordenador ubicados en distintas islas del archipiélago con un ordenador situado en Honolulu. El canal que partía de Honolulu no tenía ningún problema pues el emisor era único. Sin embargo el canal de retorno era compartido por varios emisores, por lo que había que establecer algún mecanismo que permitiera solucionar los conflictos que se producirían cuando dos emisores transmitieran simultáneamente (colisión).

La solución fue simple, los emisores transmitían sin esperar a que el canal estuviera libre. Esperaban la confirmación de llegada del mensaje, si no llegaba, suponían que había habido una colisión y volvían a enviar la trama.

Esta técnica se denominó ALOHA (saludo en hawaiano), y fue el primer protocolo de acceso al medio (MAC) que se inventó.

En 1972 fue propuesta una mejora consistente en establecer de antemano unos intervalos de tiempo de duración constante para la emisión de las tramas. De este modo las estaciones estarían sincronizadas y todas sabrían cuando empieza cada intervalo, con lo que disminuiría la probabilidad de colisión. A esta versión se la denominó ALOHA ranurado, en contraste con el anterior método conocido como ALOHA puro.

Hay un conjunto de protocolos, denominados de acceso múltiple con detección de portadora o CSMA (Carrier Sense Multiple Access), que antes de comunicar comprueban si el medio está ocupado. Esta operación permite hacer un uso más eficiente del canal y alcanzar mayores niveles de ocupación. El protocolo de este tipo que goza de mayor popularidad es el CSMA/CD (CSMA Collision Detect)

Las estaciones son capaces de detectar una colisión, lo que las hace terminar sus transmisiones inmediatamente. De este modo se ahorra tiempo y ancho de banda. Despues de detectar un choque, una estación termina su transmisión, espera un período aleatorio, y trata de emitir nuevamente.

La única circunstancia en la que puede producirse una colisión es cuando dos ordenadores empiezan a transmitir dentro de lo que se conoce como período de contienda (diferencia de tiempo entre el inicio de una transmisión y el momento en que esta transmisión habrá sido detectada por todos los equipos de la red). Para un tiempo de propagación de la señal de un extremo a otro de t , el período de contienda será de $2t$. Por este motivo, las redes CSMA/CD se suelen modelar como un sistema ALOHA rasurado con intervalos de tamaño $2t$.

Los protocolos CSMA son probabilísticas (no determinísticos) ya que la posibilidad de colisiones impide conocer cuánto tiempo puede transcurrir hasta que una estación pueda enviar una trama.

Es en este nivel donde mayor contenido presentan los protocolos al ser el desarrollado desde más antiguo. Estudiaremos los protocolos de enlace síncrono de los cuales existen dos tipos, orientados a carácter y orientados a bit.

[Bitbert-commonswiki \(CC BY-SA-2.5\)](#)

CSMA/CD (del inglés Carrier Sense Multiple Access with Collision Detection) o, en español, acceso múltiple con escucha de portadora y detección de colisiones es el estandar usado en Ethernet 802.3 en general. Se basa en que los dispositivos de red escuchan el medio antes de transmitir, es decir, es necesario determinar si el canal y sus recursos se encuentran disponibles para realizar una transmisión.

Esto solo será necesario cuando la red use **hubs** (originalmente era un cable Coaxial equivalente a un hub físico) o un **switch** solamente en sus **puertos "half-duplex"**, puesto que en los **"full-duplex"** se usan 2 pares distintos para envío y recepción de tramas entre los equipos, y por lo tanto no se pueden dar colisiones de ningún tipo.

CSMA/CA (del inglés Carrier Sense Multiple Access with Collision Avoidance) o, en español, **acceso múltiple por detección de portadora y prevención de colisiones**, es un **protocolo** de **control de acceso a redes** de bajo nivel que permite que múltiples estaciones utilicen un mismo medio de transmisión. Cada equipo anuncia opcionalmente su intención de transmitir antes de hacerlo para evitar colisiones entre los paquetes de datos (comúnmente en redes inalámbricas, ya que estas no cuentan con un modo práctico para transmitir y recibir simultáneamente). De esta forma, el resto de equipos de la red sabrán cuando hay colisiones y en lugar de transmitir la trama en cuanto el medio está libre, se espera un tiempo aleatorio adicional corto y solamente si, tras ese corto intervalo el medio sigue libre, se procede a la transmisión reduciendo la probabilidad de colisiones en el canal. CSMA/CA es utilizada en canales en los que por su naturaleza no se puede usar **CSMA/CD**. **CSMA/CA** se utiliza en **802.11** basada en **redes inalámbricas**.

5.2.5.- Protocolos orientados a carácter.

Los protocolos orientados a carácter basados en código son un tipo de protocolos utilizados en entornos síncronos y en los que la trama consta de un número entero de caracteres pertenecientes al alfabeto de un código determinado. Para efectuar el control de enlace se utilizan algunos de los caracteres del código.

Como ejemplos tenemos el BSC de IBM, el DCMP de Digital o el mismo ASCII (Código Estándar Estadounidense para el Intercambio de Información), de éste último vamos a ver algunos códigos de control:

SOH (Start Of Header): Comienzo de secuencia cabecera de mensaje.

STX/ETX (Start/End of Text): Comienzo y fin de texto.

EOT (End Of Transmision): Para marcar el final de una comunicación.

SYN (Syncronous Idle): Dos o más se utilizan como sincronización de comienzo de bloque, es la secuencia 0010110.

ACK (Afirmative Acknowledgment): Reconocimiento o acuse de recibo positivo.

NAK (Negative Acknowledgment): Reconocimiento o acuse de recibo negativo.

DEL (Data Link Escape): Es el carácter que se utiliza para cambiar el significado de los caracteres de control que le siguen.

Alfonso Bonillo - Elab.Propia (Dominio público)

Una trama básica de un protocolo orientado a carácter tiene el aspecto siguiente:

SYN	SYN	STX	MENSAJE	ETX
"Sincronizando"	"Sincronizando"	"Comienzo mensaje"	"Mensaje"	"Fin de mensaje"

Cada una de las acciones se realizan ("texto entre comillas") viene descrita por una serie de caracteres.

En este tipo de protocolos, el formato de trama es variable. Existen tramas de control y de datos.

5.2.6.- Protocolos orientados a bit.

Los protocolos basados en carácter son poco flexibles pues obligan a usar el código en que se basan (ASCII, EBCDIC...). Por este motivo aparecieron los protocolos no basados en código que, además, suelen trabajar a nivel de bit, es decir, en ellos la trama consta de un número variable de bits organizados en un conjunto fijo de campos.

Como ejemplos de protocolos de este tipo están:

HDLC (High Level Data Link Control). Familia de protocolos definida por la ISO a partir de SDLC (Synchronous Data Link Control).

LAPB (Link Access Procedure Balanced). Subconjunto de HDLC adoptado por el ITU-T para el nivel de enlace de la norma X.25.

LAPD (Link Access Procedure D-channel). Subconjunto de HDLC creado para RDSI por ITU-T. Frame Relay también utiliza una variante de LAPD.

A diferencia de los protocolos orientados a carácter, éstos utilizan una trama monoformato lo suficientemente flexible para dar servicio a todos los tipos de transmisión.

Para cubrir todas las posibles necesidades de comunicación que surjan, HDLC define:

Tres tipos de estaciones.

Estación primaria: Controla el funcionamiento del enlace. Sus tramas se denominan órdenes.

Estación secundaria: Funcionan bajo las órdenes de las estaciones primarias. Las tramas se denominan respuestas.

Estación combinada.

Dos configuraciones de enlace.

No balanceada: Una estación primaria y una o varias secundarias con transmisión semidúplex o dúplex.

Balanceada: Dos estaciones combinadas con transmisión semidúplex o dúplex.

Tres modos de operación.

NRM (Normal Response Mode): Usado en configuración no balanceada. Sólo la estación primaria puede iniciar una transmisión de datos limitándose la secundaria a responder a las órdenes de aquella. NRM se utiliza en las líneas de múltiples conexiones y, en general, cuando varios terminales se conectan a un ordenador central.

ARM (Asynchronous Response Mode): Se utiliza en configuración no balanceada permitiendo a la estación secundaria iniciar un proceso de transmisión. La estación primaria sigue siendo la responsable de la supervisión del sistema.

ABM (Asynchronous Balanced Mode): Se utiliza en la configuración balanceada. Permite que cualquier estación combinada inicie la transferencia de datos. ABM es el modo más utilizado. Usado en las redes LAN que usan tramas derivadas de HDLC. Aquí la responsabilidad del control de acceso al medio se retira de cualquier hipotética estación primaria (no existen) y se transfiere a los protocolos de control de acceso al medio (MAC).

Alfonso Bonillo - Elab.Propia (Dominio público)

Una trama HDLC tiene la forma siguiente:

INDICADOR	DIRECCIÓN	CONTROL	DATOS	FCS	INDICADOR
01111110	8 bits	8 bits	N bits	16 bits	01111110

Y podemos distinguir cuatro tipos de tramas:

Tipo 0: RECEIVE READY (ACK). Reconocimiento Positivo: RR N. Reconoce las tramas recibidas e indica que espera recibir la trama N.

Tipo 1: REJECT (NAK). Rechazo: **REJECT N.** Reconoce las tramas recibidas e indica que a partir de la trama N hay que retransmitir.

Tipo 2: RECEIVE NOT READY. Reconocimiento Positivo No Listo Para Recibir: **RNR N** Reconoce las tramas hasta la N-1 e indica que ahora mismo no puede recibir más tramas. Indica un acuse de recibo pero solicita suspensión del envío para evitar saturar al receptor (control de flujo), cosa que puede ser necesaria si el receptor tiene saturadas sus memorias temporales. Para que la retransmisión se reanude debe ser enviado un **Tipo 0**, **Tipo 1** o ciertas tramas de control.

Tipo 3: SELECTIVE REJECT. Rechazo Selectivo: **SREJ N** Indica que la trama N no llegó correctamente y debe ser retransmitida. Se utiliza para solicitar retransmisión de una trama determinada.

[Snubcube \(CC BY-SA-3.0\)](#)

Autoevaluación

La dirección física o dirección MAC es una dirección que:

- Se estudia a nivel de red.
- Está formada por 4 números.
- Se estudia a nivel enlace de datos.
- Se expresa en código octal.

NO es correcto. Deberías volver a leer el apartado.

NO es correcto. ¿Con qué criterio has optado por esta respuesta?

Correcto. A nivel enlace se identifica a los nodos con la MAC o dirección física.

NO es correcto. Quizás no has entendido la pregunta.

Solución

1. Incorrecto
2. Incorrecto
3. Opción correcta
4. Incorrecto

5.3.- Red.

El nivel de red es el encargado de identificar a cada uno de los nodos que forman parte de la red. En este nivel se describen todas las herramientas necesarias para poder identificar de manera única a cada uno de los nodos. En él se habla de direcciones de red.

El objetivo principal en este nivel es poder encaminar los paquetes desde el origen hasta el destino.

La gran decisión en el nivel de red es si el servicio debiera ser no orientado a la conexión u orientado a la conexión.

Datagramas.

Circuitos virtuales.

Ejemplos de ambos enfoques son Internet (no orientado a la conexión) y ATM (orientado a la conexión). Cuando los servicios son "no orientados" a la conexión, el nivel de red solamente garantiza que han llegado todos los datos, pero no garantiza que lleguen en el orden correcto. Cada datagrama (parte del mensaje) debe escoger su camino en cada nodo encaminador sin importarle la ruta que ha tomado otro datagrama que forma parte de un mismo paquete.

En cada nodo encaminador (router) debe existir una tabla que indique las posibles rutas que tienen que tomar los datagramas (tablas de enrutamiento).

En tecnologías que ofrecen servicios "orientados" a la conexión, primero se establece la ruta de la comunicación (circuito virtual) y después se emite. Esto permite que el emisor y el receptor se conozcan a la perfección antes de emitir y puedan negociar los parámetros de la transmisión (control de la congestión). Aquí, el orden de entrega está garantizado y por lo tanto también una "calidad en el servicio" (QoS).

Los servicios del nivel de red fueron diseñados para cumplir los siguientes objetivos:

Independencia de la tecnología empleada por debajo del nivel de red. Sea cual sea la tecnología empleada en los niveles inferiores, a nivel de red se deben entender los nodos entre sí.

El nivel de transporte no tiene por qué preocuparse de las características de las subredes. A nivel superior al de red tampoco nos debe importar lo que haya por debajo.

Las direcciones de red disponibles para el nivel de transporte han de usar un sistema uniforme. Las direcciones que se asignen a los nodos deberán seguir unos estándares que posibiliten un manejo óptimo de ellas, para poder encaminar bien los paquetes.

Uno de los protocolos más usados a nivel de red en el modelo OSI es NetBEUI (Interfaz de Usuario Extendida de NetBIOS), aunque este protocolo no funciona por defecto con los routers, es decir que no pasa de unos segmentos de red a otros por defecto, y es válido solamente en redes pequeñas (LAN), además debe actuar junto al protocolo NetBIOS.

[xcrespo11 \(CC BY-SA\)](#)

Página **36** de **83**

5.3.1.- Control de encaminamiento. Algoritmos.

El encaminamiento es el proceso mediante el cual tratamos de encontrar un camino entre dos puntos de la red: origen y destino. El objetivo consiste en tratar de encontrar la mejor ruta en la red o la ruta que tenga una métrica que más nos favorezca.

Posibles métricas son:

- Número de saltos necesarios para ir de un nodo a otro.
- Retardo de tránsito entre nodos vecinos.
- Coste económico que supone enviar un paquete de nodo a nodo.

El problema de encaminamiento diferirá según la subred sea en modo datagrama o en modo circuito virtual. En las primeras, el encaminamiento puede variar para cada paquete transmitido mientras que en modo circuito virtual el encaminamiento se decide por sesión y no se cambia a menos que sea imprescindible.

[GK tramrunner229](#) (Dominio público)

El camino óptimo también dependerá del instante en que se observa la red. Los protocolos serán los encargados de ocultar la red a sus usuarios y comprobar que las condiciones impuestas se verifican siempre. Por esta razón, el encaminamiento debe proveer a la red de mecanismos para que ésta sepa reaccionar ante variaciones del tráfico (evitar la congestión) o de topología (altas y bajas de nodos, ruptura de enlaces) y, en su caso, contribuir al mantenimiento de la QoS (Quality of Service).

Algoritmos

Para encontrar la mejor ruta entre dos puntos de la comunicación, hay que emplear técnicas y métodos que denominamos algoritmos, los principales tipos son:

- Encaminamiento salto a salto.
- Encaminamiento en origen.

Si consideramos la posibilidad de que el algoritmo reconozca en cada momento la situación de la red y pueda variar su comportamiento, la clasificación sería:

- Algoritmos adaptativos.
 - De ruta más corta (Dijkstra, Floyd-Warshall, Bellman-Ford).
 - De aprendizaje hacia atrás.
 - Centralizados.
 - Distribuidos.
 - Basados en el "vector distancia" (RIP).
 - Basados en el "estado del enlace" (OSPF).

- Algoritmos no adaptativos.
 - Estáticos.
 - Inundación.
 - Cuasiestáticos.

Para que todos estos algoritmos puedan llevarse a cabo, es necesario que cada nodo encaminador de la red posea una estructura con los siguientes elementos:

Entorno local: Información de lo que el nodo ve (memoria disponible, enlaces locales, etc.).

Alfonso Bonillo - Elab.Propia (Dominio público)

FIB (Forward Information Base): Tabla de encaminamiento que se consulta para hacer el reenvío de los PDU.

R-PDU (Routing-PDU): Paquete de control remitido por otro nodo. Contiene información de tipo variado sobre la red (nodo sigue activo, distancias a otros nodos).

RIB (Routing Information Base): Es la base de información de encaminamiento que se consulta para decidir y formar la FIBv. El nodo va acumulando en la RIB la información que obtiene a partir de la observación del entorno local y mediante la recepción de R-PDUs. A su vez, con la información almacenada en la RIB, el nodo envía R-PDUs para informar de su conocimiento del estado de la red a los demás nodos

Es decir, cada nodo encaminador debe examinar en cada momento la situación que le rodea y en base a ello tomar una decisión de la ruta óptima.

5.3.2.- Control de la congestión. Algoritmos.

La congestión se produce cuando en alguna parte de la red se da una situación en la que es imposible enviar todo lo que se recibe.

Existen varias situaciones potencialmente generadoras de congestión:

- Nodos con capacidad de proceso insuficiente.
- Velocidad insuficiente de las líneas.
- Memoria buffer insuficiente en los conmutadores.

Es distinto el control de flujo (nivel enlace) que el control de la congestión. El control de congestión es un concepto

Alfonso Bonillo - Elab.Propia (Dominio público)

más amplio que el control de flujo. Comprende todo un conjunto de técnicas para detectar y corregir los problemas que surgen cuando no todo el tráfico ofrecido a una red puede ser cursado. Es un concepto global que involucra a toda la red, y no sólo a un remitente y un destinatario de información, como es el caso del control de flujo. El control de flujo es una de las técnicas para combatir la congestión.

Algoritmos

Existen varios algoritmos que ayudan a reducir la congestión, las dos técnicas principales se basan en vigilar el tráfico e intentar reconducirlo y controlarlo para que no se sature ningún nodo o directamente, descartar aquellos paquetes que saturan el sistema (más radical).

La clasificación sería la siguiente:

- Conformación y vigilancia del tráfico.
- Algoritmo del cubo agujereado.
- Algoritmo del cubo con cupones.
- Control de subredes virtuales.
- Paquetes reguladores.
- Descarte de paquetes.

Alfonso Bonillo - Elab.Propia (Dominio público)

5.4.- Transporte.

El objetivo principal de este nivel es proporcionar un transporte de datos confiable de la máquina origen a la máquina destino, independientemente del medio físico utilizado; se pretende que para establecer una sesión de comunicación a este nivel no debe importarnos nada más que la dirección origen y la dirección destino.

A nivel de red, los usuarios de a pie no tienen control sobre el funcionamiento del servicio ya que toda la gestión se lleva en los puntos de conexión y enrutamiento, por lo que el nivel transporte pretende añadir mejoras que resuelvan posibles problemas en el servicio. Todo el software a nivel de transporte se ejecuta en las máquinas de los usuarios.

Este nivel es el límite entre el proveedor de servicios y el usuario, en el se habla de términos como **puertos** y **sockets**.

Cuando un proceso de aplicación quiere establecer comunicación con otro proceso de aplicación remoto, debe especificar a cuál se conectará. El método que normalmente se emplea es el de definir direcciones de transporte en las que los procesos pueden estar a la escucha de solicitudes de conexión. Estos puntos terminales se llaman **puertos** (en ATM se llaman **AAL-SAPs**). También se pueden denominar **TSAP** (Punto de Acceso al Servicio de Transporte).

Para el caso del nivel de red, **NSAP** (Punto de Acceso al Servicio de Red) es lo mismo que decir dirección **IP**.

A veces los servicios tienen **TSAP** estables que se listan en archivos en lugares bien conocidos (etc/services de Unix que lista cuáles servidores están enlazados de manera permanente a cuáles puertos).

No es rentable tener **TSAP** estables porque puede haber puertos que se utilicen muy pocas veces, lo ideal sería que todas las aplicaciones pudieran usar todos los puertos posibles. Por otra parte, hay determinadas aplicaciones que necesitan tener un puerto identificado con un número que no varíe (puertos bien conocidos).

En lugar de que cada servidor concebible escuche en un **TSAP** bien conocido, cada máquina que desee ofrecer servicio a usuarios remotos tiene un **Servidor de Procesos** especial que actúa como proxy de los servidores de menos uso.

Este servidor escucha en un grupo de puertos al mismo tiempo, esperando una solicitud de conexión.

Los usuarios potenciales de un servicio comienzan por emitir una solicitud **CONNECT**, especificando la dirección **TSAP** del servicio que desean. Si no hay ningún servidor esperándolos, consiguen una conexión al servidor de procesos. El servidor de procesos les asigna un **TSAP** y vuelve a la escucha.

5.5.- Sesión. Funciones.

El nivel sesión es el encargado de controlar la comunicación entre las aplicaciones, se dice que controla el diálogo entre aplicaciones de diferentes máquinas para que el transporte de datos sea óptimo. A este nivel se intercambian "datos".

A nivel sesión se establecen comunicaciones proceso a proceso en red entre los distintos hosts. Para que haya comunicación entre dos host de la red es necesario que se establezca una "sesión" entre ellos, antes de empezar a transmitir.

La capa sesión es un concepto que aparece por primera vez con OSI. La capa sesión tiene como misión permitir a sus usuarios (que pueden ser entidades de la capa de presentación o de la capa de aplicación) establecer conexiones, denominadas sesiones, para la transferencia de datos ordenada. Por ejemplo, una sesión podría utilizarse para un acceso desde un ordenador personal a una base de datos remota.

Usualmente, cuando se solicita que la capa de sesión establezca una sesión, con carácter previo se deberá haber establecido una conexión de transporte sobre la que fluirá la sesión. Esta conexión de transporte puede ser monosesión o utilizarse consecutivamente, para más de una sesión.

[Gmelander \(CC BY-SA-4.0\)](#)

Funciones

Sus funciones son bastante reducidas consistiendo fundamentalmente en permitir la transferencia de datos, controlar el orden de intervención de los interlocutores en ciertos diálogos (provocar un funcionamiento consulta-respuesta en los accesos a una base de datos), facilitar la vuelta a un estado anterior tras un problema (sincronizar un proceso) y en resumen permitir al usuario el establecimiento de sesiones de comunicación en las cuales puede transmitir datos a través del sistema.

Actuar de interfaz entre el usuario y la red, gestionando el establecimiento de la conexión entre procesos de hosts remotos.

Negociar la forma en que se intercambian los datos dos equipos remotos.

Identificar los usuarios de los host remotos.

Restablecer las comunicaciones rotas a nivel transporte.

Alfonso Bonillo - Elab.Propia (Dominio público)

Página **40** de **83**

5.6.- Presentación.

Este nivel es el responsable de codificar los datos para que la comunicación entre los host sea homogénea. Recibe los datos de la capa aplicación en forma de texto, imagen, sonido, instrucción y los transforma para poder generar datos con estructuras similares que se puedan transformar mejor. Por ejemplo, cuando hacemos una mudanza, se pueden transportar mejor las cosas si van metidas en cajas de tamaño homogéneo (se pueden colocar mejor en el medio de transporte) que si las llevamos sueltas, se aprovecha mejor el espacio, se optimiza el medio de transporte y su manejo es más fácil.

Entre los códigos que nos podemos encontrar en este nivel se encuentran EBCDIC, ASCII y UNICODE. A este nivel también aparecen los mecanismos de seguridad y encriptación (firma electrónica) de datos.

Dos tareas complementarias de este proceso de traducción son la compresión y el cifrado de los datos. Con ellos se pretende, por un lado, eliminar de los mensajes por transmitir aquellos componentes superfluos que luego pueden ser añadidos directamente en el extremo receptor y, por otro, enmascarar la información transmitida de modo que un hipotético escucha del sistema de comunicación no pueda recuperar el mensaje original sin conocer el código de descifrado.

No hay ningún impedimento a la existencia de un cifrado de nivel de presentación por un lado, y de un cifrado de nivel aplicación por otro.

[Wilinckx](#) (Dominio público)

Debes conocer

Te recomendamos que revises estos conceptos:

EBCDIC (*Código de intercambio decimal de código binario extendido*)
ASCII (*Código Estándar Estadounidense para el Intercambio de Información*)
UNICODE (*código uniforme, universal y único*)

5.7.- Aplicación.

La capa de aplicación contiene los **protocolos que usarán los programas** de usuario (aplicaciones) que hacen el trabajo real para el que fueron adquiridos los ordenadores (crear textos online, chatear, leer correo, visitar webs).

Esta capa es la que entra en contacto con las aplicaciones de los usuarios finales. Tiene la particularidad de que incluye cualquier función o servicio que se use en la red y que no se suministre en los niveles anteriores/inferiores. Es posible escribir un libro con miles de páginas con la multitud de cosas útiles que hace el nivel de aplicación.

[wilgengebroed \(CC BY-NC\)](#)

Debes conocer

Uno de los protocolos más típico de esta capa es el HTTP (o HTTPS para usar comunicaciones seguras mediante SSL) que permite a los clientes web o clientes de HTTP o navegadores web (Firefox, Chrome, etc.) comunicarse e intercambiar páginas web (escritas en lenguaje de marcas HTML) y todo tipo de contenido con los servidores web o servidores HTTP (como por ejemplo Apache, NGINX, IIS, etc.) que escuchan por defecto en el puerto 80 (ó 443 para HTTPS).

Funciones

Entre los cometidos más importantes de este nivel figuran:

Compresión de la información transmitida.

El coste de utilización de una red de comunicaciones suele ser fuertemente dependiente, en sentido directamente proporcional, de la cantidad de datos transmitidos. Así pues, una forma de reducir dicho coste sería conseguir que la información que se envía por la red ocupase el menor volumen posible. Para ello y manteniendo constantes el resto de parámetros, no hay nada mejor que utilizar las técnicas de compresión.

La compresión de la información se utiliza intensivamente para ahorrar recursos, sean estos, espacio de memoria secundaria, o ancho de banda en comunicaciones. Esta técnica requiere dos algoritmos paralelos pero no necesariamente simétricos, el de compresión y el de descompresión. Respecto a ellos es importante diferenciar entre compresión de datos y compresión multimedia.

En la compresión de datos se exige que lo que se comprimió, sea exactamente lo que se descomprime (sin pérdidas).

En la compresión multimedia no suele ser necesario que al descomprimir se obtenga una imagen perfecta de lo que se codificó (con pérdidas). Se admite una degradación que hace que el proceso sea más rápido.

Alfonso Bonillo - Elab.Propia (Dominio público)

Ejemplo de compresión de datos es el formato conocido como mp3.

Seguridad y confidencialidad.

La seguridad no era algo que preocupara excesivamente a los primeros usuarios de las redes de comunicaciones, usando éstas para poco más que enviarse correo electrónico y compartir alguna impresora dentro de una universidad u organización cerrada, pocos problemas de este tipo podían producirse.

Hoy en día, el panorama ha cambiado, las organizaciones que desean utilizar el correo electrónico y los demás servicios de Internet, bien internamente, bien para relacionarse con el exterior, deben tomar medidas que permitan garantizar la confidencialidad, la integridad y la disponibilidad de la información.

Existen cuatro conceptos básicos en seguridad que son:

- 1.- **Control de integridad:** ausencia de modificación o destrucción no autorizadas de la información.
- 2.- **Disponibilidad/no repudio:** consiste en impedir la denegación no autorizada de acceso a la información.
- 3.- **Segreto/confidencialidad:** supone evitar la divulgación no autorizada de la información.
- 4.- **Validación de identificación/autenticación:** busca la seguridad en el proceso de dar y reconocer la autenticidad de la información y/o la identidad de los actores y/o el permiso por parte de los autorizadores.

Es en este apartado donde se deben abordar los temas relacionados con la criptología, que se divide en dos ciencias antagonistas: la criptografía y el criptoanálisis. Estas ciencias son las encargadas de diseñar todas las técnicas utilizadas para encriptar los datos enviados de un usuario a otro a través de la red.

Gestión de red: SNMP.

El objetivo genérico de un sistema de gestión de red es proporcionar una plataforma de gestión distribuida para todo tipo de entornos de red.

El estándar de gestión más utilizado actualmente es el denominado SNMP, que incluye un protocolo de gestión (RFC 1157), una especificación de estructura de base de datos de información de gestión (MIB) y un conjunto de definiciones de objetos de datos permitidos (RFC 1155). La versión SNMP v2, soporta TCP/IP y OSI. SNMP no proporciona gestión de red sino un marco de trabajo sobre el que se pueden construir aplicaciones de gestión de red.

Gestión y conversión de nombres de dominio: DNS.

Conjunto de protocolos y servicios sobre una red TCP/IP, que permite a sus usuarios utilizar nombres jerárquicos sencillos, en lugar de sus direcciones IP, para comunicarse con otros equipos.

Si no existiera la funcionalidad DNS, tendríamos que saber cada una de las direcciones únicas de cada elemento de la red, para poder visualizar la página www.openoffice.org tendríamos que poner en el explorador <http://95.216.24.32>. Sería imposible recordar todas y cada una de las direcciones de todos los portales que quisiéramos visitar.

Antes de la implantación de DNS, la traducción de direcciones IP a nombres de computadoras se efectuaba mediante listas de nombres y sus direcciones IP asociadas, almacenados en archivos hosts.txt.

Estos archivos contenían el nombre y la dirección asociada a ese nombre, de manera que cuando yo quiero conectarme con un host no necesito recordar su dirección, recurro al fichero y en ese fichero busco la dirección que corresponde a ese nombre; es más fácil recordar un nombre que 4 números.

DNS está compuesto de una base de datos distribuida de nombres que se organiza según una estructura lógica arborescente conocida como espacio de nombres de dominio.

Cada nodo o dominio en el DNS tiene un nombre y puede, a su vez, contener subdominios.

Los dominios y subdominios se agrupan en zonas que permiten la administración distribuida del espacio de nombres.

Cada dominio se nombra por la trayectoria desde él hasta la raíz (que no tiene nombre) separando cada nivel jerárquico con un punto.

La raíz de la base de datos de DNS en Internet es administrada por el InterNIC. Los nombres de dominios siguen el estándar internacional ISO 3166.

Cuando un usuario desea crear un portal y asignarle un determinado nombre, por ejemplo hola.adios, debe "pedir permiso" a InterNIC para saber si ese nombre está o no permitido y disponible. Hay muchas empresas que se dedican a proporcionar el servicio de alojamiento ("hosting") a cambio de dinero, pero también hay posibilidad de tener un nombre en Internet de manera gratuita (<https://www.paginawebgratis.es/>).

Esta mecánica de asignar nombres para poder identificar ciertos host en Internet hizo que en su día, usuarios demasiado avisados registraran nombres asociados a marcas de bebidas, ropa o aparatos electrónicos impidiendo que esas compañías pudieran utilizarlos, provocando que tuvieran que desembolsar grandes cantidades de dinero para poder utilizar los nombres asociados a sus marcas.

[Josef Sábl \(CC BY-SA\)](#)

Para saber más

Te recomendamos leer el siguiente enlace sobre el formato de compresión de audio MP3.

[¿Cómo funciona la compresión MP3?](#)

6.- El modelo TCP/IP.

Caso práctico

La instalación de una sala de formación con ordenadores en red no tiene mucha complicación y hay momentos en los que cada uno tiene claro cuál debe ser su cometido que repercute en el trabajo del compañero que le sigue. En ese momento se encuentra el grupo de **BK Sistemas Informáticos** con **Vindio** y **Laro** como responsables, y **Naroba**, **Noiba** y **Jara** como ayudantes aprendiendo de la experiencia.

En un momento que coinciden, **Naroba** comenta que es complicado entender que el modelo de red que se viene utilizando es el TCP/IP y sin embargo se estudia en todos los casos el modelo OSI.

Vindio responde que aunque las similitudes son muy claras parece que desde el punto de vista académico se insiste en estudiar ambos sistemas, algo muy coherente ya que es necesario conocer las particularidades de cada modelo, en especial si quieras optar a uno de los muchos cursos de certificación que requiere el sector de los profesionales de sistemas en general y redes en particular.



Alain Bachellier (CC BY-NC-SA)

TCP/IP se suele confundir muchas veces con un protocolo de comunicaciones concreto, cuando, en realidad, es una compleja arquitectura de red que incluye varios de ellos, apilados por capas. Es, sin lugar a dudas, la más utilizada del mundo, ya que es la base de comunicación de Internet y también se utiliza ampliamente en las distintas versiones de los sistemas operativos Unix y Linux (aunque debido a su gran utilización ha sido también implantado en otros sistemas como Windows).

En el año 1973, el DoD (Departamento de Defensa de Estados Unidos) inició un programa de investigación para el desarrollo de tecnologías de comunicación de redes de transmisión de datos. El objetivo fundamental era desarrollar una red de comunicación que cumpliera las siguientes características:

Permita interconectar redes diferentes. Esto quiere decir que la red en general puede estar formada por tramos que usan tecnología de transmisión diferente.

Sea tolerante a fallos. El DoD deseaba una red que fuera capaz de soportar ataques terroristas o incluso alguna guerra nuclear sin perderse datos y manteniendo las comunicaciones establecidas. Permita el uso de aplicaciones diferentes: transferencia de archivos, comunicación en tiempo real, etc.

Todos estos objetivos implicaron el diseño de una red con topología irregular donde la información se fragmentaba para seguir rutas diferentes hacia el destinatario. Si alguna de esas rutas fallaba repentinamente, la información podría seguir rutas alternativas. Así, surgieron dos redes distintas: una dedicada a la investigación, ARPANET, y otra de uso exclusivamente militar, MILNET.

El DoD permitió a varias universidades que colaboraran en el proyecto, y ARPANET se expandió gracias a la interconexión de esas universidades e instalaciones del Gobierno. Este modelo se nombró después como arquitectura TCP/IP, por las iniciales de sus dos protocolos más importantes. En 1980, TCP/IP se incluyó en Unix 4.2 de Berkeley y fue el protocolo militar estándar en 1983. En ese mismo año nació la red global Internet, que utiliza también esta arquitectura de comunicación. ARPANET dejó de funcionar oficialmente en 1990.

Algunos de los motivos de la popularidad alcanzada por esta arquitectura son:

Es independiente de los fabricantes y las marcas comerciales.

Soporta múltiples tecnologías de redes.

Es capaz de interconectar redes de diferentes tecnologías y fabricantes.

Puede funcionar en máquinas de cualquier tamaño, desde ordenadores personales a grandes supercomputadores.

Se ha convertido en estándar de comunicación en EEUU desde 1983.

La arquitectura de TCP/IP se construyó diseñando inicialmente los protocolos para, posteriormente, integrarlos por capas en la arquitectura. Por esta razón, a TCP/IP muchas veces se la califica como pila de protocolos. Su modelo por niveles es algo diferente a OSI de ISO, como demuestra la tabla siguiente.

Capas según el modelo OSI		Capas según el modelo DoD (TCP/IP)	
7	Aplicación <i>Application</i>	4	Aplicación <i>Process</i>
6	Presentación <i>Presentation</i>		
5	sesión <i>Session</i>		
4	Transporte <i>Transport</i>	3	Transporte <i>Host-to-Host</i>
3	Red <i>Network</i>	2	Internet <i>Network</i>
2	Enlace de datos <i>Data Link</i>	1	Acceso al medio <i>Media Access</i>
1	Física <i>Physical</i>		

Obsérvese que TCP/IP sólo tiene definida 4 capas, que cubren las funcionalidades de los siete niveles del modelo OSI. Las funciones que realizan cada una de ellas son las siguientes:

1.- Capa de acceso a la red o acceso al medio: el modelo no da mucha información de esta capa, y solamente se especifica que debe existir algún protocolo que conecte la estación con la red. La razón fundamental es que, como TCP/IP se diseñó para su funcionamiento sobre redes diferentes, esta capa depende de la tecnología utilizada y no se especifica de antemano.

2.- Capa de internet (o de red): esta capa es la más importante de la arquitectura y su misión consiste en permitir que las estaciones envíen información (paquetes) a la red y los hagan viajar de forma independiente hacia su destino. Durante ese viaje, los paquetes pueden atravesar redes diferentes y llegar desordenados. Esta capa no se responsabiliza de la tarea de ordenar de nuevo los mensajes en el destino, pero sí de intentar evitar congestiones en la red. El protocolo más importante de esta capa se llama IP (Internet Protocol), aunque también existen otros protocolos en ella.

3.- Capa de transporte: ésta cumple la función de establecer una conversación entre el origen y el destino, dotando de fiabilidad a la comunicación, encargándose de la ordenación de los paquetes y de sus posibles pérdidas. Aquí también se han definido varios protocolos, entre los que destacan TCP (Transmission Control Protocol), orientado a la conexión y fiable, y UDP (User Datagram Protocol), no orientado a la conexión y no fiable.

4.- Capa de aplicación: esta capa contiene, todos los protocolos de alto nivel que utilizan los programas para comunicarse. Aquí se encuentra el protocolo de terminal virtual (TELNET), el de transferencia de archivos (FTP), el protocolo HTTP que usan los navegadores en la World Wide Web, los protocolos de gestión del correo electrónico, etc.

Las capas de sesión y presentación no existen en la arquitectura TCP/IP, ya que los diseñadores pensaron que no se necesitaban. La experiencia obtenida con los trabajos realizados en el modelo OSI ha comprobado que esta visión fue correcta: se utilizan muy poco en la mayoría de las aplicaciones de comunicación. En caso de que, por ejemplo, alguna aplicación desee utilizar un servicio de encriptación de datos o recuperación ante caídas, será necesario incluirlos dentro del propio programa de

aplicación.

Aplicación	Usuario	Desde aquí hacia arriba mira hacia el usuario
Transporte	Es el primer nivel que ve la conexión "de Extremo a Extremo"	
Red	Rutas	
Enlace	Nodo inmediatamente Adyacente	
Físico	Aspectos Mecánicos, físicos y eléctricos (u ópticos)	



Acorletti, [TCP-IP red y aplicación \(CC BY-SA\)](#)

Para saber más

En el siguiente videotutorial se explica algunas características de la arquitectura TCP/IP:

[Arquitectura TCP/IP](#)

6.1.- Capa de Subred.

En el nivel subred se estudia todo lo relativo a los parámetros físicos de la red, lo que en el modelo OSI engloba en el nivel Físico. Se estudiarán todas las características físicas de los medios de transmisión.

Como quiera que el modelo TCP/IP no contempla un nivel intermedio que le separe del nivel Internet, en este nivel se estudiarán los protocolos de acceso al medio entre otros que el modelo OSI trata en el nivel enlace.

Lo más cercano a un protocolo de nivel enlace en TCP/IP es el protocolo de subred. Consiste en dos capas (IMP). Su objetivo consiste en proporcionar una capa fiable para la transmisión de tramas de un IMP a sus vecinos inmediatos.

Un caso particular de nivel enlace en Internet es el que ataña al transporte de tramas IP sobre líneas serie. Su importancia es cada vez mayor ya que se aplica a las conexiones temporales de Internet entre PC de usuarios y los proveedores de servicios de Internet.

Los dos protocolos más característicos son SLIP y PPP.

SLIP – SERIAL LINE IP

Este es el más antiguo de los protocolos y data de 1984. Se trata de un protocolo muy sencillo que utiliza un carácter como indicador, y caracteres de relleno en caso de que dicho carácter aparezca en la trama. Solo se utiliza en comunicaciones conmutadas.

SLIP no es capaz de detectar tramas erróneas. Su uso ha decaído a favor de PPP.

PPP (POINT TO POINT PROTOCOL)

PPP se ha diseñado para ser muy flexible, para lo cual incluye un protocolo especial, denominado LCP (protocolo de control de enlace), que se ocupa de negociar (handshaking) una serie de parámetros en el momento de establecer la conexión con el sistema remoto.

La estructura de la trama PPP se basa en la de HDLC (control de enlace de datos de alto nivel), aunque se trata de un protocolo orientado a carácter. La trama tiene la siguiente estructura:

Indicador	Dirección	Control	Protocolo	Datos	Verificación	Indicador
01111110	11111111	00000011	Protocolo	Variable	CRC	01111110

El campo dirección no se utiliza, siempre vale todo 1. Ello se debe a que las conexiones son siempre punto a punto y, por lo tanto, no tiene sentido utilizar dirección alguna.

El campo control contiene siempre el valor 00000011, que indica una trama no numerada. Por defecto PPP no suministra transmisión fiable (con números de secuencia y acuse de recibo como HDLC).

LCP negocia siempre la supresión de los bytes dirección y control de la trama al inicio de la sesión cuando no se pide transmisión fiable.

El campo protocolo establece a qué tipo de protocolo pertenece el paquete recibido de la capa de red. PPP permite establecer una comunicación multiprotocolo, puede utilizarse para transmitir paquetes pertenecientes a diferentes protocolos del nivel de red entre dos ordenadores.

LCP también suministra mecanismos que permiten validar al ordenador que llama (claves usuario/contraseña).

PPP es un mecanismo de transporte de tramas multiprotocolo que puede utilizarse sobre medios físicos muy diversos, por ejemplo, conexiones módem y RTC, RDSI, líneas dedicadas, o incluso

por conexiones SONET/SDH de alta velocidad.

Alfonso Bonillo-Elab.Propia (Dominio público)

Página **44** de **83**

6.2.- Capa de Internet.

El nivel de red en el modelo TCP/IP se suele denominar capa de red o capa IP y es el nivel donde se acepta o transfieren las tramas.

Este nivel está determinado por las características del protocolo IP, definido en un documento público RFC 791.

En la siguiente figura se puede ver un paquete IP (en verde) que encapsula un segmento TCP o UDP (morado) que encapsula a algún paquete de datos de alguna aplicación:

Alfonso Bonillo-Elab.Propia (Dominio público)

Para saber más

Si tienes curiosidad por conocer ese documento, puedes consultar el siguiente enlace:

[Documento RFC 791](#)

6.2.1.- Formato de Paquete IP.

Toda la información en una red IP ha de viajar en datagramas IP, comúnmente llamados paquetes IP.

El tamaño máximo de un datagrama IP es de 65535 bytes, a repartir entre encabezado y texto. Se trata de un valor teórico que no se utiliza en la práctica. Normalmente, el nivel de red adapta el tamaño de cada paquete para que viaje en una trama de enlace de la red utilizada.

Un paquete IP tiene el siguiente aspecto:

Versión	IHL	Tipo de Servicio			Longitud Total							
Identificación	F	DF	MF	Desplazamiento del Fragmento								
Tiempo de Vida	Protocolo		Suma de Verificación del Encabezado									
Dirección de Origen												
Dirección Destino												
Opciones												

Versión: IPv4 ó IPv6. Permite que coexistan tramas con diferentes versiones de paquetes IP.

IHL: Longitud en palabras de 32 bits del encabezamiento.

Tipo de servicio.

Longitud total del datagrama.

Identificación: Determina a que datagrama pertenece el fragmento. Todos los fragmentos de un datagrama incluyen la misma identificación.

DF: Orden a todos los routers de que no fragmenten el datagrama, ya que el destino no puede montarlo de nuevo.

MF: Todos los fragmentos, salvo el último de un datagrama tienen este bit activado.

Desplazamiento del fragmento: A que parte del datagrama pertenece este fragmento. El tamaño del fragmento elemental es de 8 bytes. Todos los fragmentos excepto el último han de tener un tamaño múltiplo del tamaño elemental.

Tiempo de vida o Time To Live (TTL): En IPv6 le han dado un nombre mejor de "Hop limit". Es un valor de 8 bits que se inicializa en el origen del paquete y después cada vez que llega a un router se reduce una unidad. Se utiliza para ir descontando saltos. Cuando llega a cero, el paquete se descarta y se envía al host origen un aviso. Se usa en los "traceroute".

Protocolo: Protocolo de capa de transporte al que debe entregar el datagrama. Comúnmente será TCP o UDP.

Suma de comprobación: Aritmética de complemento a 1 para controlar la producción de errores en la cabecera.

Direcciones IP de origen y destino.

Opciones: Incluyen el encaminamiento en origen estricto, el encaminamiento libre desde el origen, la grabación de la ruta, la **marca de tiempo** y la seguridad.

[Appaloosa \(CC BY-SA\)](#)

Página **46** de **83**

6.2.2.- Direcciones IPv4.

Las direcciones IP públicas de Internet se asignan de forma única y centralizada, pero delegando por territorios.

Históricamente se ha ido realizando de diversas formas y por distintos organismos, [InterNIC](#) ([Internet Network Information Center](#)) fue el principal organismo gubernamental de internet responsable de los [nombres de dominio](#) y las [Direcciones IP](#) hasta el 18 de septiembre de 1998, cuando este papel fue asumido por la [Internet Corporation for Assigned Names and Numbers](#) (ICANN).

A día de hoy, La Corporación de Internet para la Asignación de Nombres y Números ([ICANN](#)) delega los recursos de Internet a los Registros Regionales de Internet ([RIR](#)), y a su vez los RIR siguen sus políticas regionales para una posterior subdelegación de recursos a sus clientes, que incluyen proveedores de servicios de Internet ([ISP](#)) y organizaciones para uso propio.

Una dirección [IPv4](#) consta de **32 bits**, agrupados de 8 en 8 y representados en **4 números de código decimal**. Los valores de estos 4 números decimales van **entre 0 y 255**.

Las direcciones IP pueden **clasificarse** en función de quién las asigna y dónde:

Públicas (válidas y únicas en Internet).

Privadas (válidas solamente a nivel local de una organización, son únicas a nivel local, pero no se pueden usar en la parte pública de Internet y tendrán que ser convertidas a públicas mediante [NAT](#) que se verá en la última unidad del curso).

También se pueden clasificar las direcciones IP en función de si son asignadas de forma permanente o temporal:

[Skyrocket2005](#). Direcciones IP de clase A, B y C, con sus partes de red y estación. (Dominio público)

Estáticas (no cambian con el tiempo).

Dinámicas (puede cambiar su valor cuando ha pasado un intervalo de tiempo determinado).

Otra clasificación posible sería en función de si se **asignan** de forma:

Manual (mediante una persona que administre/configure el equipo y la asigne).

Automáticas (el dispositivo hace una petición automática a un servidor [DHCP](#) que le asigna una IP de un determinado rango, junto con otros datos necesarios como su máscara de subred, su puerta de enlace predeterminada y su servidor de nombres de dominio).

Aunque normalmente las direcciones IP se representan en decimal para que los humanos las entendamos mejor, de manera interna el dispositivo informático siempre las trata en forma binaria para trabajar con ellas, y además también será necesario para identificar algunas de sus características de red, por ejemplo:

Convertir la siguiente dirección IP en binario a decimal: 10001111010101100011110101100001

Solución: 143.86.61.97

Cómo se puede ver, se podrían identificar hasta 2^{32} (4.294.967.296) direcciones IP distintas combinando los 32 bits, aunque no se puedan utilizar todas para identificar equipos como veremos más adelante.

Una dirección IP consta de los siguientes campos y surge la siguiente clasificación:

IDENTIFICADOR (TIPO) + NUMERO DE RED + NUMERO DE ESTACION

Clase de IP	Bits iniciales en el primer octeto, Identificadores de la Clase	Número de bits que restan para identificar la parte de red	Número de bits para identificar la parte de estación
A	0	7 bits	24 bits
B	10	14 bits	16 bits
C	110	21 bits	8 bits
D	1110	28 bits	-
E	1111	28 bits	-

Clase	Rango de IPs	Número de redes posibles de esa clase	Número máximo de estaciones por cada red (restando 2 para la dirección de red y la de broadcast)
A	0.0.0.0 - 127.255.255.255	$2^7 = 128$	$2^{24} - 2 = 16777214$
B	128.0.0.0 - 191.255.255.255	$2^{14} = 16384$	$2^{16} - 2 = 65534$
C	192.0.0.0 - 223.255.255.255	$2^{21} = 2097152$	$2^8 - 2 = 254$
D	224.0.0.0 - 239.255.255.255	-	-
E	240.0.0.0 - 255.255.255.255	-	-

DIRECCIONES RESERVADAS y/o ESPECIALES:

De todas las direcciones IP, hay algunas que no se pueden utilizar porque están reservadas para el uso del protocolo IP y tienen una consideración "especial" como:

0.0.0.0: Tiene varios usos como se puede ver en [Wikipedia](#). Puede representar tanto "todas las IPs" como "ninguna" según el contexto. También se utilizaba cuando se están arrancando las estaciones, hasta la carga del sistema operativo, luego no se usa. Antiguamente se usaba también cuando no se obtenía una dirección mediante DHCP, pero ahora se usa [APIPA](#) en sistemas operativos Windows entre otros. **Todo el rango de IPs que comienza con el primer octeto a 0 está reservada.**

127.0.0.1: Para especificar la estación actual, cuando se desea especificar el ordenador local (**localhost**). Todo el rango de IPs que comienza en el primer octeto por 127 está reservada al mismo propósito, es decir que en cualquier equipo que tenga su pila de protocolos TCP/IP instalada en el sistema operativo podrá hacer ping a la 127.0.0.1 o la 127.0.0.2 o la 127.22.22.22 y el ping debe responder positivamente.

Dirección con **todos los bits a 0** en la parte de "host": Representa a la subred actual y no puede ser asignada por tanto a ningún equipo.

Dirección con **todos los bits a 1** en la parte de "host": Difusión (broadcast) en su subred. Para enviar mensajes a todas las estaciones dentro de la misma subred (todas las estaciones con los mismos bits en la parte de red de su IP). Por lo tanto tampoco podrá ser asignada a ningún equipo de la subred.

No hay que confundir las direcciones de difusión (**broadcast**) de las subredes (para enviar mensajes a las estaciones de la misma subred) con las direcciones de la clase D, que más bien, se utilizan para agrupar estaciones en un mismo grupo/canal de multicast y enviarlas mensajes de multi-difusión o **multicast** (pueden pertenecer a redes o subredes distintas).

Además de las direcciones **reservadas** anteriores, se han establecido otros rangos de direcciones IP para ser asignados a redes locales **privadas**, que cuando se conectan a Internet a través de un proxy o mediante un router/encaminador que use un protocolo NAT serán convertidas a una (o varias) **IPs públicas**.

Clase	Rangos Reservados y Especiales
A	<p>0.0.0.0 - 0.255.255.255 : reservado</p> <p>10.0.0.0 - 10.255.255.255 : reservado para redes internas/privadas</p> <p>127.0.0.0 - 127.255.255.255 – reservado para direcciones tipo loopback, solo a nivel interno del propio dispositivo</p>
B	<p>169.254.0.0 – 169.254.255.255 : Direcciones usadas por APIPA cuando falla el DHCP</p> <p>172.16.0.0 - 172.31.255.255 : reservado para redes internas/privadas</p>
C	192.168.0.0 - 192.168.255.255 : reservado para redes internas/privadas

Debes conocer

Esta clasificación de direcciones IP según su clase es importante conocerla, aunque a día de hoy se usa más bien el concepto de Máscaras de Subred de Longitud Variable o CIDR (Classless InterDomain Routing) que permite una mejor segmentación y aprovechamiento de las escasas IPs públicas.

El concepto de "máscara de subred" (y la diferencia entre red y subred) **se verá en unidades posteriores**, y por ahora está bien saber que la Máscara de subred "por defecto" de una dirección IP estará relacionada con la clase de IP que se tenga.

Para saber más

Esta calculadora de subredes online tiene mucha utilidad e información adicional. Los ejercicios y cálculos de subredes IP los veremos en profundidad en la siguiente unidad.

[Calculadora de subredes](#)

Recomendación

Estos vídeos te pueden ayudar a comprender mejor estos conceptos tan importantes:

- 1.- [Direccionamiento IPv4 y Subredes](#)
- 2.- [Curso de Redes de AulaClic. 8.4 Direcciones IP y enrutamiento en un host.](#)

6.2.3.- Protocolos relacionados con IP.

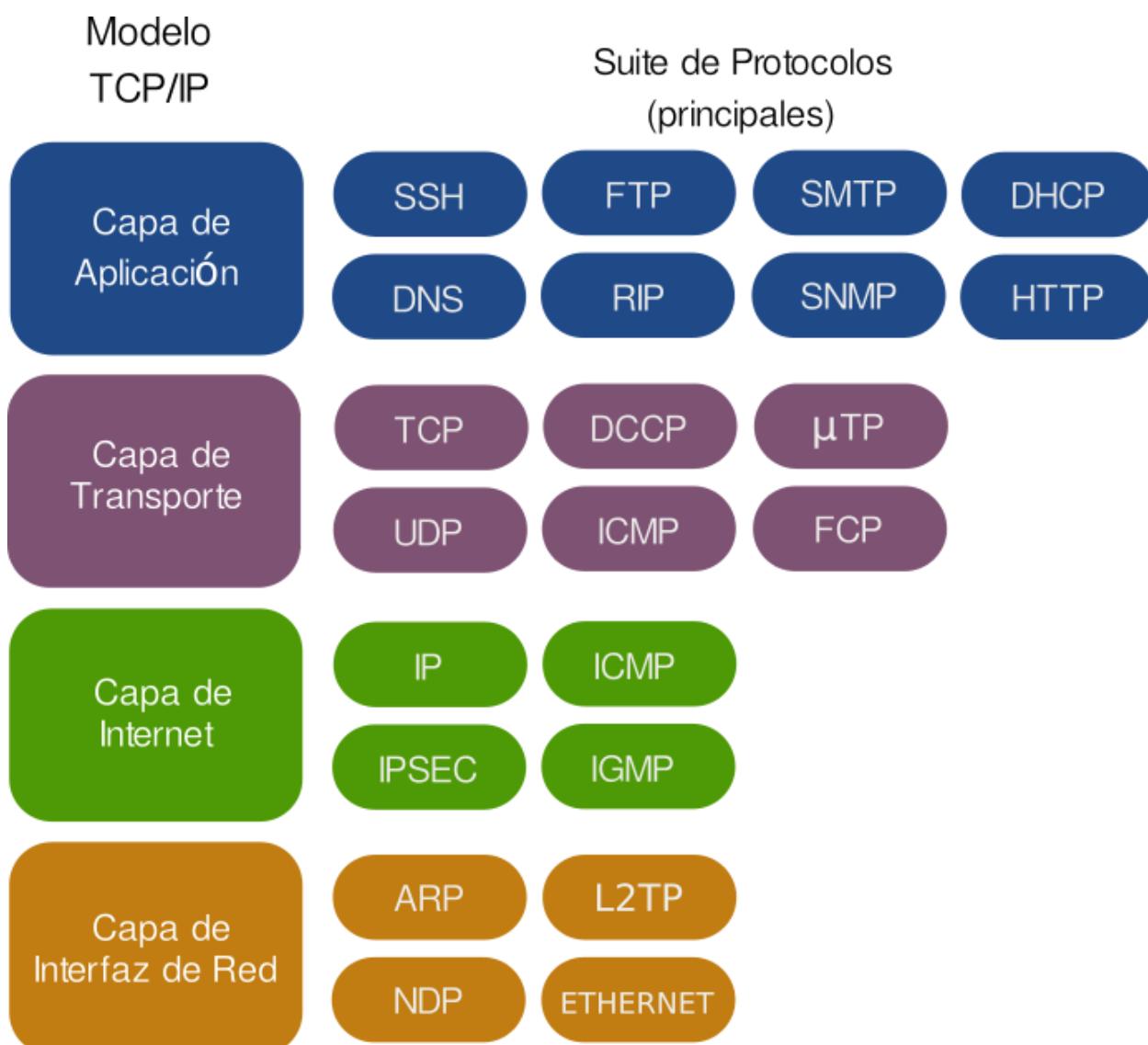
Existen una serie de protocolos que están estrechamente relacionados con el protocolo IP, los más conocidos son:

ARP: Es un protocolo capaz de encontrar la dirección física (MAC) si se le proporciona la dirección IP correspondiente.

RARP: Es capaz de realizar el camino inverso a ARP, encontrar la IP a partir de la dirección física.

ICMP: Es el responsable de enviar al usuario los errores que proporciona una determinada aplicación sobre el sistema operativo. Es el protocolo que usan las herramientas "ping" y "traceroute".

IGMP: Protocolo responsable de los mensajes a los miembros de un grupo de **multicast** en una red de tipo LAN.



[GISEPROI. Suite de Protocolos TCPIP \(CC BY-SA\)](#)

Alfonso Bonillo-Elab.Propia. *Proceso de encapsulamiento* (Dominio público)

Página 48 de 83

6.3.- Capa de Transporte.

El nivel transporte, tal como se ilustra en la figura que representa la comunicación entre los niveles OSI, es el primer nivel en el que dejamos de preocuparnos por las características de los nodos intermedios entre el emisor y el receptor. El nivel transporte en el modelo TCP/IP viene determinado por las características de los dos protocolos más importantes TCP y UDP.

La capa de transporte añade la noción de puerto para distinguir entre los muchos destinos dentro de un mismo host. No es suficiente con indicar la dirección IP del destino, además hay que especificar la aplicación que recogerá el mensaje. Cada aplicación que esté esperando un mensaje utiliza un número de puerto distinto; más concretamente, la aplicación está a la espera de un mensaje en un puerto determinado (escuchando un puerto).

Pero no sólo se utilizan los puertos para la recepción de mensajes, también para el envío: todos los mensajes que envíe un ordenador debe hacerlo a través de uno de sus puertos.

Cuando se habla de "abrir puertos", a lo que realmente nos referimos es a ejecutar aplicaciones que usan un determinado puerto, con lo que conseguimos tener ese puerto activo y listo para enviar o recibir datos.

Un puerto es un número de 16 bits, por lo que existen 65536 puertos en cada ordenador. Las aplicaciones utilizan estos puertos para recibir y transmitir mensajes.

Los números de puerto de las aplicaciones cliente son asignados dinámicamente y generalmente son superiores al 1024. Cuando una aplicación cliente quiere comunicarse con un servidor, busca un número de puerto libre y lo utiliza. En cambio, las aplicaciones servidoras utilizan unos números de puerto prefijados: son los llamados puertos well-known ("bien conocidos"). Puertos conocidos son 80 (HTTP), 21 (FTP), 23 (TelNet).

Los puertos tienen una memoria intermedia (buffer) situada entre los programas de aplicación y la red. De tal forma que las aplicaciones transmiten la información a los puertos. Aquí se va almacenando hasta que pueda enviarse por la red. Una vez que pueda transmitirse, la información irá llegando al puerto destino donde se irá guardando hasta que la aplicación esté preparada para recibirla.

6.3.1.- Protocolos: UDP y TCP.

Protocolo UDP

Es un protocolo de la capa transporte cuya principal característica es la de que no es orientado a la conexión.

Este protocolo proporciona una comunicación muy sencilla entre las aplicaciones de dos ordenadores. Al igual que el protocolo IP de la capa de red, este protocolo es "no confiable", es decir, los datos pueden llegar dañados. Utiliza a IP para transportar sus mensajes, la PDU (o datagrama) que en esta capa se llama "**segmento**" es parecida a la de IP pero incorpora el puerto origen y el puerto destino. Este protocolo solo sirve para aplicaciones que no necesiten garantías en la comunicación. Esto es muy práctico en aplicaciones en que es más importante la velocidad de transmisión (como comunicación de audio y vídeo: IPTV, VoIP, juegos en línea) o en aplicaciones servidoras sin estado que deben responder pequeñas consultas de un gran número de clientes (como DNS). A diferencia de TCP, UDP permite paquetes de difusión (broadcast y multicast).

[Anónimo \(CC0\)](#)

Esto es muy práctico en aplicaciones en que es más importante la velocidad de transmisión (comunicación de audio y vídeo, VoIP, juegos en línea) o en aplicaciones servidoras sin estado que deben responder pequeñas consultas de un gran número de clientes (DNS). A diferencia de TCP, UDP permite paquetes de difusión (broadcast y multicast).

Protocolo TCP

Es un protocolo de la capa transporte cuya principal característica es la de que es orientado a la conexión. Se diseñó precisamente para proporcionar un servicio confiable sobre una red no confiable. Es decir, es necesario establecer una comunicación previa entre emisor y receptor antes de transmitir los datos. Además el uso de este protocolo nos asegura que los datos recibidos son exactamente los datos enviados.

Para que esta comunicación pueda ser posible es necesario abrir previamente una conexión. Esta conexión garantiza que los todos los datos lleguen correctamente de forma ordenada y sin duplicados.

Cada byte no se envía inmediatamente después de ser generado por la aplicación, sino que se espera a que haya una cierta cantidad de bytes, se agrupan en un segmento y se envía el segmento completo. Para ello son necesarias unas memorias intermedias o buffers.

Cada uno de estos segmentos viaja en el campo de datos de un datagrama IP. Si el segmento es muy grande será necesario fragmentar el datagrama, con la consiguiente pérdida de rendimiento; y si es muy pequeño, se estarán

[Anónimo \(CC0\)](#)

enviando más cabeceras que datos. Por consiguiente, es importante elegir el mayor tamaño de segmento posible que no provoque fragmentación.

La carga útil de IP es de 65515 bytes, el segmento TCP debería tener ese tamaño, pero en la práctica sucede que cada red tiene una unidad máxima de transferencia (**MTU**), en redes Ethernet el tamaño de la carga útil es de 1500 bytes.

El formato de un segmento TCP sería de la siguiente forma:

Puerto TCP Origen	Puerto TCP Destino
Número de Secuencia	
Número de Acuse de Recibo NUMERO DE ACUSE DE RECIBO	
HLEN	Reservado
Suma de Verificación	Puntero
Opciones	Relleno
Datos	
...	
...	

6.3.2.- Conexiones / Sockets.

Una conexión está formada por el par **dirección IP + puerto**. No puede haber dos conexiones iguales en un mismo instante pero sin embargo en mismo ordenador si puede tener dos conexiones distintas utilizando un mismo puerto. A estas conexiones se las llama **SOCKET**.

Un **socket** es por tanto una dirección de Internet que combina:

una dirección **IP** (la dirección numérica única de cuatro partes que identifica a un ordenador particular en Internet) y
un número de puerto (número que identifica una aplicación de Internet particular):

21	-	FTP
22	-	FTPS / SSH
80	-	HTTP
110	-	POP3
143	-	IMAP
443	-	HTTPS
993	-	IMAP SSL
995	-	POP3 SSL

Para saber más

La definición de [Network Socket](#) en la wikipedia da más información interesante y particularizada.

Puedes ver los sockets abiertos en tu PC con el comando "netstat" en Windows.

6.4.- Capa de Aplicación.

Este nivel engloba a todos aquellos protocolos que están más cerca del usuario final. Los protocolos pertenecientes a esta capa son los más conocidos por todos los usuarios (HTTP, FTP, SMTP, DNS).

La diferencia con el nivel aplicación de OSI, es que aquí las capas sesión, presentación y aplicación se funden todas en una. Esto provoca que haya protocolos y servicios que según el modelo TCP/IP se sitúan en al mismo nivel y que tienen pocas cosas en común. Por otra parte, se consigue que no haya niveles que como en el caso del modelo OSI aparezcan casi vacíos.

[Brivadeneira \(CC BY-SA-4.0\)](#)

Debes conocer

Uno de los protocolos más típicos de esta capa es el HTTP (o HTTPS para usar comunicaciones seguras mediante SSL) que permite a los clientes web o clientes de HTTP o navegadores web (Firefox, Chrome, etc.) comunicarse e intercambiar páginas web (escritas en lenguaje de marcas HTML) y todo tipo de contenido con los servidores web o servidores HTTP (como por ejemplo Apache, NGINX, IIS, etc.) que escuchan por defecto en el puerto 80 (ó 443 para HTTPS).

Autoevaluación

El modelo TCP/IP triunfó sobre el OSI porque:

- Se implantó antes.
- Por las IP.
- Se crearon protocolos que se utilizaban de inmediato.
- Era más académico.

No es correcto. Deberías volver a leer los apartados anteriores.

No es correcto. Recomendamos que vuelvas a leer los apartados.

Correcto. Los protocolos TCP/IP se utilizaban antes de estandarizarse como TCP/IP.

No es correcto. Ese no es motivo suficiente.

Solución

1. Incorrecto
2. Incorrecto
3. Opción correcta
4. Incorrecto

7.- Redes LAN: Ethernet y Wi-Fi

Caso práctico

Vindio explica que las diferentes formas de realizar la conexión de una red local se reducen a la correspondiente configuración de los dispositivos de conexión, principalmente los switchs, porque aunque existen diferentes modos de organizar la red, en **BK Sistemas Informáticos** siempre utilizan estos dispositivos para instalar y configurar las redes locales.

Una vez hecha la conexión existen una gran variedad de configuraciones posibles según las necesidades de cada cliente. En este caso la conexión Ethernet parece la más adecuada y por la que vamos a optar.



Alain Bachellier (CC BY-NC-SA)

En este apartado nos centraremos en las redes más usadas en este curso, las redes locales. Existen multitud de estándares y protocolos de redes locales, entre las que podemos destacar: las redes Ethernet, WiFi, FDDI y las redes Token Ring, **éstas dos últimas ya en desuso**.

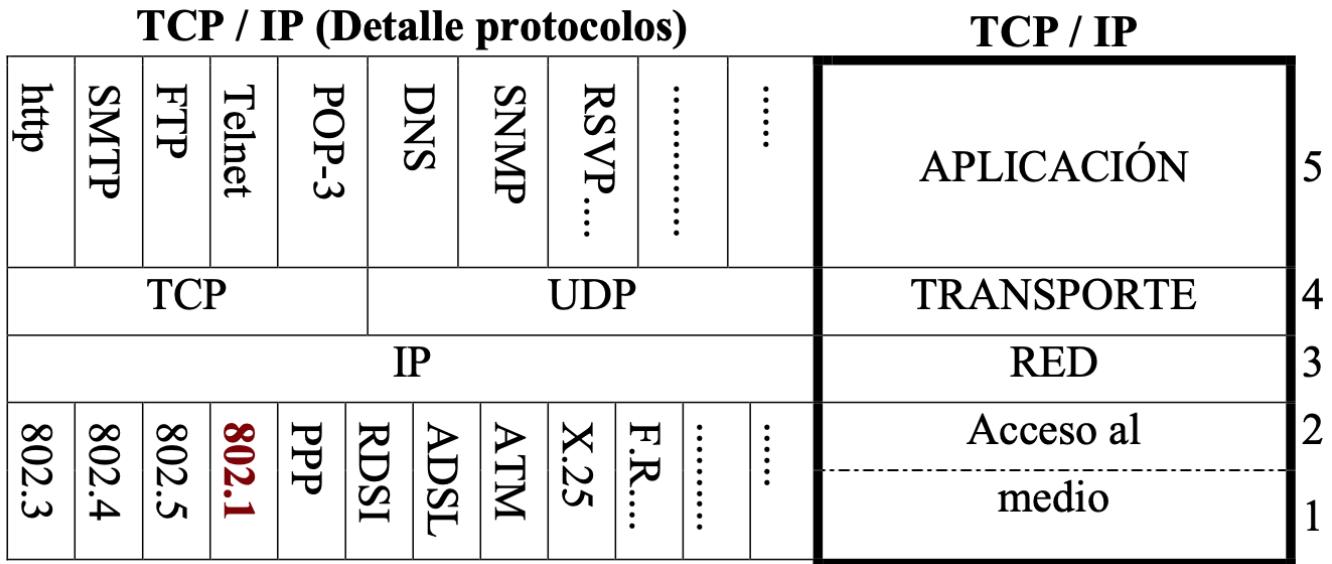
La arquitectura de las redes locales sigue un esquema parecido que la arquitectura TCP/IP original, pero se añadieron pequeñas diferencias que afectan principalmente a la capa de enlace de datos. Esta capa, como ya sabemos, proporciona fiabilidad en el intercambio de tramas entre las estaciones: básicamente control de errores y control de flujo. Pero por el hecho de usar un medio compartido, en las redes locales será necesario establecer mecanismos para que todas las estaciones puedan usar dicho medio sin molestararse.

Si dos estaciones ponen tramas (o paquetes) en el medio de transmisión de forma simultánea, éstas se mezclarán de manera que se convertirán en algo ininteligible. Esta situación se conoce como colisión de tramas, necesitándose mecanismos para controlar el acceso al medio compartido, de manera que no se produzcan, o que si se producen, la red pueda recuperarse y seguir funcionando. Estos mecanismos se incluyeron en el modelo TCP/IP, para redes locales, dividiendo la capa de enlace de datos en dos subniveles:

LLC (logical link control o control del enlace lógico), que se encarga de los servicios típicos de enlace: **control de errores y control de flujo**. En general esta capa será **independiente** del tipo de cableado de red que se tenga (coaxial, par trenzado de diversas categorías, fibra óptica, etc.). Las características de esta parte se encuentran recogidas en el estándar **IEEE 802.2**.

MAC (medium access control o control de acceso al medio), que se encarga propiamente de la política de acceso al medio y sí dependerá del medio físico (cableado) del que disponga nuestra red.

Las características de esta parte se encuentran recogidas en los estándares desde el **IEEE 802.3** al **IEEE 802.12**. Cada uno de ellas establece un tipo de red local diferente, que resultan incompatibles entre sí.



[Acorletti, Pila TCP/IP y algunos de los protocolos que la componen \(CC BY-SA\)](#)

Como hemos referido anteriormente, entre las redes locales destacan:

Las redes Ethernet.- Es el estándar predominante de redes locales y en ellas centraremos la mayor parte de nuestro curso. El primer estándar de Ethernet fue diseñado en 1976 por Xerox y, posteriormente, revisado por Intel, DEC y Xerox; permitiendo una velocidad de transmisión de **10 Mbps**. Más adelante se adaptó para ser compatible con el estándar **IEEE 802.3**, que fue elaborado en 1990 por la organización IEEE (Institute of Electrical and Electronics Engineers o Instituto de Ingenieros Eléctricos y Electrónicos) para la comunicación en redes locales. Dentro de este estándar se han definido varios tipos de redes locales en lo que se refiere al tipo de cableado utilizado, velocidad de transmisión, formato de los bloques de información enviados, reparto del medio, etc. Por ejemplo tenemos el **10BASE2**, **1000BASE-T**, **10GBASE-T**, etc. y que veremos más adelante.

Ethernet utiliza el protocolo de acceso al medio **CSMA/CD** en el que las estaciones están permanentemente a la escucha del canal y, cuando lo encuentran libre de señal, efectúan sus transmisiones inmediatamente. Esto puede llevar a una colisión que hará que las estaciones suspendan sus transmisiones, esperen un tiempo aleatorio y vuelvan a intentarlo.

Cualquier estación conectada a una red IEEE 802.3 debe poseer una tarjeta de red que cumpla con este estándar y con los componentes electrónicos y el software adecuado para la generación y recepción de tramas.

La tarjeta o adaptador de red se encarga de verificar las tramas que le llegan desde el canal, así como de **ensamblar** los datos de información dándoles la forma de una trama, detectar los posibles errores en destino, etc. La tarjeta también es la encargada de negociar los recursos que necesita con el sistema operativo del ordenador en que se instala.

Las redes Token Ring.- En su momento fue un método popular para conectar redes locales, aunque ya prácticamente ha desaparecido en favor del estándar Ethernet. Usan el estándar **IEEE 802.5**. Su principal característica es que, aunque utiliza una topología física en forma de estrella, ésta funciona como una estructura **lógica en anillo**. Esto se consigue gracias a la utilización de un concentrador de cableado llamado MAU (Unidad de Acceso Multiestación) como nodo central de la estrella.

Las redes Wi-Fi.- Son redes locales inalámbricas que siguen el estándar **IEEE 802.11**, transmiten datos a través de ondas de radio a una velocidad que depende de la versión utilizada (1,5 Mbps es la primera versión, de 5,5 a 11 Mbps en el estándar IEEE 802.11b o 54 Mbps en el estándar **IEEE 802.11g**). Algunos adaptadores que siguen el estándar IEEE **802.11ac** pueden llegar hasta 1,3 Gbps. Este tipo de redes se clasifica como LAN, ya que habitualmente se instala dentro del ámbito de un edificio. Su topología está distribuida en emisores y receptores de ondas de radio que están conectados entre sí y dispersados por toda la organización. De esta forma, cualquier equipo que disponga también de un emisor y receptor estará permanentemente conectado en cualquier lugar, sin necesidad de utilizar cables.

Las redes Wi-Fi comparten ciertas partes del protocolo Ethernet como las **direcciones MAC** para identificar a nivel de capa 2 a todas las estaciones de la red únicamente.

En el resto de capas superiores (de 3 a 7) todas las redes en general comparten los mismos protocolos.

Las redes inalámbricas (Wi-Fi y otras) se verán en profundidad en la unidad 2.

7.1.- La historia de Ethernet.

Conocemos a Ethernet como la tecnología que está definida en el estándar IEEE 802.3. Hoy en día es la tecnología que proporciona conectividad en las redes LAN a casi el 98% de los equipos del mundo.

Las variantes de Ethernet tienen la misma arquitectura de acceso al medio múltiple con detección de errores, CSMA/CD (Carrier Sense Multiple Access with Collision Detection).

Sin embargo, el estándar IEEE 802.3 ha evolucionado de forma que ahora soporta múltiples medios en la capa física, incluyendo cable coaxial, cable par trenzado sin blindaje (Unshielded Twisted Pair o UTP), cable par trenzado con blindaje (Shielded Twisted Pair o STP) y fibra óptica.

[Anónimo \(CC BY\)](#)

Su nombre se debe a "Luminiferous ether" (éter luminífero). En un tiempo se pensó que la radiación electromagnética se propagaba a través de él. En el siglo XIX Maxwell descubrió que la radiación electromagnética se podría describir mediante una ecuación de onda, los científicos supusieron que el espacio debía estar lleno de algún medio etéreo en el cual se propagaba la radiación, después se descubrió que la radiación electromagnética se podía propagar en el vacío.

En 1972 en PARC (Centro de Investigación de Xerox en Palo Alto) se diseñaba lo que se consideraba la 'oficina del futuro', se estaban probando unos ordenadores denominados Alto, que disponían de capacidades gráficas y ratón y son considerados los primeros ordenadores personales, también se estaban fabricando las primeras impresoras láser.

Se quería conectar los ordenadores entre sí para compartir ficheros y las impresoras. La comunicación tenía que ser de muy alta velocidad, del orden de megabits por segundo, ya que la cantidad de información a enviar a las impresoras era enorme (tenían una resolución y velocidad comparables a una impresora láser actual). Estas ideas que hoy parecen obvias eran completamente revolucionarias en 1973.

A Metcalfe, el especialista en comunicaciones del equipo con 27 años de edad, se le encomendó la tarea de diseñar y construir la red que uniera todo aquello. Contaba para ello con la ayuda de un estudiante de doctorado de Stanford llamado David Boggs. Las primeras experiencias de la red, que denominaron 'Alto Aloha Network', las llevaron a cabo en 1972. Fueron mejorando gradualmente el prototipo hasta que el 22 de mayo de 1973 Metcalfe escribió un memorándum interno en el que informaba de la nueva red. Para evitar que se pudiera pensar que sólo servía para conectar ordenadores, Alto cambió el nombre inicial por el de Ethernet, que hacía referencia a la teoría de la física hoy ya abandonada según la cual las ondas electromagnéticas viajaban por un fluido denominado éter que se suponía llenaba todo el espacio (Metcalfe llamaba éter al cable coaxial por el que iba la portadora).

La red de 1973 ya tenía todas las características esenciales de la Ethernet actual. Empleaba CSMA/CD para minimizar la probabilidad de colisión, y en caso de que ésta se produjera ponía en marcha el mecanismo de retroceso exponencial binario para reducir gradualmente la 'agresividad' del emisor, con lo que éste se autoadaptaba a situaciones de muy diverso nivel de tráfico. Tenía topología de bus y funcionaba a 2,94 Mbps sobre un segmento de cable coaxial de 1,6 Km de longitud.

Las direcciones eran de 8 bits y el CRC de las tramas de 16 bits. El protocolo utilizado a nivel de red era el PUP (Parc Universal Packet) que luego evolucionaría hasta convertirse en el actual XNS (Xerox Network System).

En 1977 Metcalfe, Boggs y otros dos ingenieros de Xerox recibieron una patente por la tecnología básica de Ethernet, y en 1978 Metcalfe y Boggs recibieron otra por el repetidor. En esta época todo el sistema Ethernet era propietario de Xerox.

Ethernet usaba topología en bus con cable coaxial en sus inicios, hoy en día lo más normal es encontrarse una topología física en estrella con cable de par trenzado.

[Asim18 \(CC BY-SA\)](#)

Para saber más

[Vídeo sobre la historia de Ethernet](#) contado por su creador (en inglés subtitulado español).

7.2.- Medios de transmisión. El cableado Ethernet.

Caso práctico

Laro tiene que realizar la conexión de todos los equipos a la red mediante una serie de "latiguillos" o cables de red que van desde cada ordenador a un conector de la canaleta que recorre la pared de la sala que será la nueva sala de formación de la empresa.

La empresa tiene claro que el mejor modo de llevar a cabo esta tarea debe ser cortando los cables al tamaño necesario en cada momento para después crimpar los conectores, creando de ese modo los "latiguillos" exactos que necesitamos y la adecuada longitud de cable empleado.

En el Instituto hizo muchas prácticas de creación de cables de diferentes tamaños y tiene claro que el secreto está en utilizar las herramientas adecuadas y de buena calidad. Una máquina de crimpado defectuosa supone el desperdicio de cable.



[Alain Bachelier \(CC BY-NC-SA\)](#)

Como ya hemos visto, en sus orígenes Ethernet utilizaba cable coaxial grueso y topología en bus, hoy en día el tipo de cable más utilizado en estas redes es el cable de par trenzado que incluye varios tipos. De hecho, si nos referimos a un cable como "cable Ethernet", la mayoría de la gente piensa en un cable de par trenzado y casi nunca en un cable coaxial.

[Tseppelt \(CC BY-SA-4.0\)](#)

Medios de transmisión físico

En un sistema de transmisión denominamos medio de transmisión al soporte físico mediante el cual el emisor y el receptor establecen la comunicación. Los medios de transmisión se clasifican en guiados y

no guiados. En ambos casos la transmisión se realiza mediante ondas electromagnéticas. En el caso de los medios guiados estas ondas se conducen a través de cables.

La velocidad de transmisión, el alcance y la calidad (ausencia de ruidos e interferencias) son los elementos que caracterizan a los medios guiados. La evolución de la tecnología en lo que respecta a los cables ha estado orientada por la optimización de estas tres variables.

1.- **Velocidad de transmisión**, en la actualidad las velocidades alcanzadas difieren notablemente entre los diferentes tipos de cables, siendo la fibra óptica la que permite alcanzar una velocidad mayor.

2.- **Alcance de la señal**, está determinado por la atenuación que sufre dicha señal según va circulando por el cable y que es mayor cuanta más distancia debe recorrer, por lo que este factor limita considerablemente la longitud de cable que se puede instalar sin regenerar la señal.

3.- **Calidad de la señal**, uno de los principales problemas de la transmisión de un flujo de datos por un cable eléctrico consiste en el campo magnético que se genera por el hecho de la circulación de los electrones. Este fenómeno es conocido como inducción electromagnética. La existencia de un campo magnético alrededor de un cable va a generar interferencias en los cables próximos debido a este mismo fenómeno.

7.2.1.- Cableado coaxial.

Las primeras redes de tipo Ethernet tenían un cableado coaxial con topología en bus. Este tipo de red está formada por varios equipos unidos entre sí mediante un cable coaxial. Para unir cada equipo al cable se utilizan las conexiones tipo "T".

Además, en los extremos del cable se utilizan "terminadores" que se unen a un extremo de la "T" de los ordenadores de los extremos de la red. Si por alguna causa el cable se rompe, la red deja de funcionar.

El cable coaxial más utilizado en la actualidad es el **RG-59** de 75 Ω de impedancia también llamado cable coaxial de banda ancha, que no es ni más ni menos que el cable coaxial utilizado para televisión y redes de cable (CATV o televisión por cable).

- A: Cubierta protectora de plástico
- B: Conductor blindado de malla de aluminio revestido de cobre
- C: Aislante (o dieléctrico)
- D: Conductor central o núcleo (acero revestido de cobre)

[Ari - Wikimedia \(CC BY-SA-3.0\)](#)

El cable coaxial es similar al cable utilizado en las antenas de televisión: un hilo de cobre en la parte central rodeado por una malla metálica y separados ambos elementos conductores por un cilindro de plástico, protegidos finalmente por una cubierta exterior.

La denominación de este cable proviene de que los dos conductores comparten un mismo eje de forma que uno de los conductores envuelve al otro.

La malla metálica exterior del cable coaxial proporciona una pantalla para las interferencias. En cuanto a la atenuación, disminuye según aumenta el grosor del hilo de cobre interior, de modo que se consigue un mayor alcance de la señal.

Los tipos de cable coaxial para las redes de área local son:

1.- **Thicknet** (Ethernet grueso): Tiene un grosor de 1,27 cm y capacidad para transportar la señal a más de 500 m. Al ser un cable bastante grueso se hace difícil su instalación por lo que está prácticamente en desuso. Fue el primer cable montado en redes Ethernet. Este cable se corresponde con el estándar RG-8/U, posee un característico color amarillo con marcas cada 2,5 m que designan los lugares en los que se pueden insertar los ordenadores.

2.- **Thinnet** (Ethernet fino): Tiene un grosor de 0,64 cm y capacidad para transportar una señal hasta 185 m. Posee una impedancia de 50 ohmios. Es un cable flexible y de fácil instalación (comparado con el cable coaxial grueso). Se corresponde con el estándar **RG-58** y puede tener su núcleo constituido por un cable de cobre o una serie de hilos de cobre entrelazados.

El cable coaxial es menos susceptible a interferencias y ruidos que el cable de par trenzado y puede ser usado a mayores distancias que éste. Puede soportar más estaciones en una línea compartida. Es un medio de transmisión muy versátil con un amplio uso. Los más importantes son:

- 1.- Redes de área local.
- 2.- Transmisión telefónica de larga distancia.
- 3.- Distribución de televisión a casas individuales (televisión por cable).

Transmite señales analógicas y digitales, su frecuencia y velocidad son mayores que las del par trenzado.

El gran inconveniente de este tipo de cable es su grosor, superior al del cable de par trenzado, lo que dificulta mucho su instalación, encareciendo ostensiblemente el coste por mano de obra. De ahí, que pese a sus ventajas, en cuanto a velocidad de comunicación y longitud permitida, no se presente de forma habitual en las redes de área local.

Los elementos necesarios para la conexión del cable coaxial pertenecen a la familia denominada BNC. Los principales son:

- 1.- **Conecotor BNC**, en forma de T, conecta la tarjeta de red del ordenador con el cable de red.
- 2.- **Terminador**, se trata de una resistencia de 50 ohmios que cierra el extremo del cable. Su finalidad es absorber las señales perdidas, y así evitar que reboden indefinidamente.
- 3.- **Conecotor acoplador**, denominado barrel, utilizado para unir dos cables y así alargar su longitud.

Para saber más

Para conocer algo más sobre el cable coaxial te recomendamos que visites el siguiente enlace:

[Cable Coaxial](#)

7.2.2.- Cableado de par trenzado.

Lo que se denomina **un par trenzado** consiste en dos alambres de cobre aislados, que **se trenzan de forma helicoidal**, igual que una molécula de ADN. De esta forma el par trenzado constituye un circuito que puede transmitir datos.

Esto se hace porque dos alambres paralelos constituyen una antena simple. Cuando se trenzan los alambres, las ondas de diferentes vueltas se cancelan, por lo que la radiación del cable es menos efectiva. Así la forma trenzada permite reducir la interferencia eléctrica tanto exterior como de pares cercanos.

Un **cable de par trenzado** está formado por un grupo de pares trenzados, **normalmente cuatro**, recubiertos por un material aislante.

Cada uno de estos pares se identifica mediante un color, siendo los colores asignados y las agrupaciones de los **4 pares (8 hilos)** de la siguiente forma:

- Par 1: Blanco-Azul/Azul
- Par 2: Blanco-Naranja/Naranja
- Par 3: Blanco-Verde/Verde
- Par 4: Blanco-Marrón/Marrón

Los pares trenzados se apantallan. De acuerdo con la forma en que se realiza este **apantallamiento** podemos distinguir varios tipos de cables de par trenzado, éstos se denominan mediante las siglas **UTP**, **STP** y **FTP**.

UTP (Unshielded Twisted Pair) es como se denominan a los cables de par trenzado no apantallados (o no blindados), son los más simples, no tienen ningún tipo de pantalla conductora. Es muy sensible a interferencias. Los pares están recubiertos de una malla de teflón que no es conductora. Este cable es bastante **flexible y barato** por lo que es el más usado.

STP (Shielded Twisted Pair) es la denominación de los cables de par trenzado apantallados individualmente, cada par se envuelve en una malla conductora y otra general que recubre a todos los pares. Poseen gran inmunidad al ruido, pero una **rigidez máxima**.

En los cables **FTP** (Foiled Twisted Pair) los pares se recubren de una malla conductora global en forma trenzada. De esta forma mejora la protección frente a interferencias, teniendo una **rigidez intermedia**.

Dependiendo del número de pares que tenga el cable, del número de vueltas por metro que posea su trenzado y de los materiales utilizados, los estándares de cableado estructurado clasifican a los cables de pares trenzados por **categorías**: 3, 4, 5, 5e, 6 y 7.

Categoría 3: soporta velocidades de transmisión hasta **10 Mbps**.

Categoría 4: soporta velocidades hasta 16 Mbps.

Categoría 5: hasta **100 Mbps**.

Categoría 5 mejorada (5e o 5 enhanced): En esta versión se mejoran los parámetros del cable para llegar hasta transmisiones de **Gigabit Ethernet (1000 Mbps)**.

Categoría 6: Mejora las características de la 5e. Tiende a sustituirla.

El cable de Par Trenzado debe emplear **conectores RJ-45** para unirse a los distintos elementos de hardware que componen la red. Cada conector **depende de la categoría del cable** que se vaya a utilizar, por lo tanto, al adquirirlos se debe especificar la categoría del cable que se pretende utilizar con ellos.

Las redes Ethernet actuales utilizan el cable de par trenzado y suelen tener una topología en estrella (un switch en el centro conectando a todos los equipos (ordenadores, otros switches, routers, etc.) . Este tipo de cableado ha ganado terreno respecto al cableado coaxial o la fibra por su instalación y coste.

A pesar de que con pares trenzados se ha conseguido transmitir incluso a velocidades superiores al Gbps, sus 2 verdaderas limitaciones son el **alcance** (entre 10m y 100m en función de su categoría y la velocidad permitida) y su sensibilidad a las **interferencias** electro-magnéticas. En casos de necesitar mayores alcances o evitar posibles interferencias se opta por usar pares de fibra óptica.

[Dmitry G \(CC BY-SA\)](#)

[Mozzerati \(CC BY-SA\)](#)

[Chunait \(CC BY-SA-3.0\)](#)

[Interiot-commonswiki](#) (Dominio público)

Herramienta crimpadora para colocar los conectores RJ45 en un cable de pares trenzados.

Importante: **¡¡¡no hay que pelar los cables!!!**

Autoevaluación

¿Qué se logra mediante el trenzado de los alambres en un cable CAT-5?

- El cable queda más delgado.
- Es más económico.
- Limita la degradación de la señal.
- Permite que 6 pares quepan en el espacio de 4 pares.

Incorrecta, piensa un poco, ¿quedá más delgado?

NO, el trenzado encarece el cable.

Correcto. Al trenzarse los filamentos por pares se reducen las interferencias internas.

Incorrecto, me tienes que explicar cómo se consigue eso.

Solución

1. Incorrecto
2. Incorrecto
3. Opción correcta
4. Incorrecto

Para saber más

Para un técnico de sistemas es muy importante conocer cómo crear un cable de conexión, en [este video](#) podrás aclarar muchas dudas y aprender a construirlo.

Además recomendamos el siguiente enlace por la información adicional que aporta para el conexionado del cable UTP con conector RJ45, donde explica las dos terminaciones posibles T568A y T568B.

[Cable de Par trenzado con RJ45](#)

También te puede resultar interesante para saber cómo se realiza el crimpado del cable en conectores RJ45 el siguiente enlace.

[Crimpado de cable Ethernet RJ45](#)

7.2.3.- Fibra Óptica.

La fibra óptica está basada en la utilización de ondas de luz para transmitir información binaria.

Un sistema de transmisión óptico se compone de tres componentes:

La fuente de luz: convencionalmente, un pulso de luz indica un bit 1 y la ausencia de luz un bit 0.

El medio de transmisión: fibra de vidrio ultradelgada.

El detector: genera un impulso eléctrico cuando la luz incide sobre él.

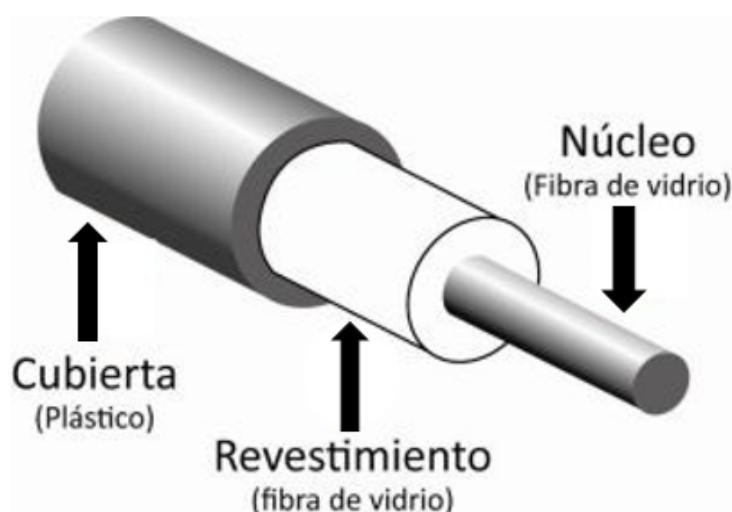
Al agregar una fuente de luz en un extremo de la fibra óptica y un detector en el otro extremo disponemos de un sistema de transmisión de datos **unidireccional**. Por eso hace falta al menos un **par** de fibras por conexión, para enviar y recibir información.



[Asurnipal](#). Par de fibras con conectores SC (CC BY-SA)

El medio de transmisión consiste básicamente en dos cilindros coaxiales de vidrios transparentes y de diámetros muy pequeños. El cilindro interior se denomina **núcleo** y el exterior se denomina **revestimiento**, siendo el índice de refracción del núcleo algo mayor que el del revestimiento. En la superficie de separación entre el núcleo y el revestimiento se produce un fenómeno de reflexión total de

la luz. La **envoltura**, al poseer un menor índice de refracción mantiene toda la luz en el interior. Finalmente una **cubierta** plástica delgada (o envoltura) impide que cualquier rayo de luz del exterior penetre en la fibra. Varias fibras suelen agruparse en haces protegidos por una funda exterior.



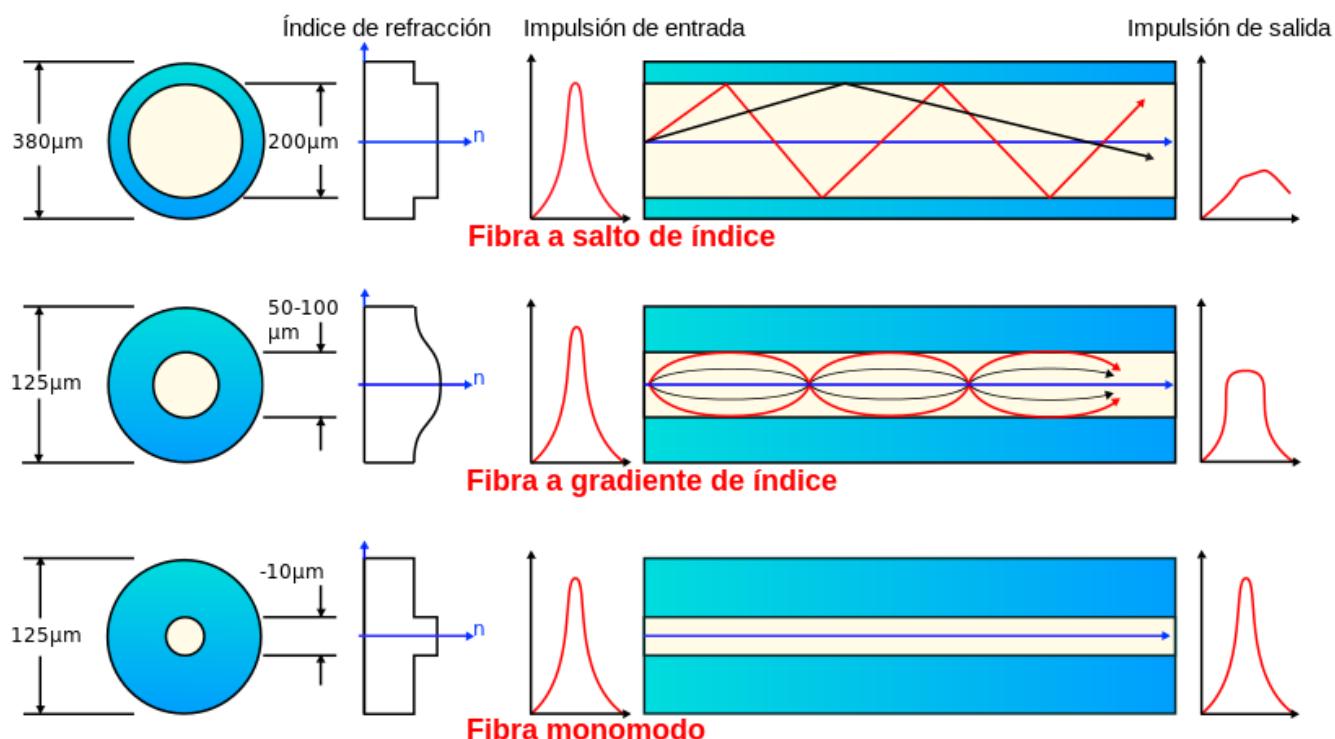
[Rafavg. Partes de la fibra \(CC BY-SA\)](#)

Existen tres formas diferentes de transmisión de la luz:

Monomodo: En este caso la fibra es tan delgada que la luz se transmite en línea recta. El núcleo tiene un radio de $10 \mu\text{m}$ y el revestimiento de $125 \mu\text{m}$. Su cubierta suele ser de color amarillo.

Multimodo: La luz se propaga por el interior del núcleo incidiendo sobre su superficie interna, como si se tratara de un espejo. El núcleo tiene un radio de $100 \mu\text{m}$ y el revestimiento de $140 \mu\text{m}$. Su cubierta suele ser de color naranja.

Multimodo de índice gradual: La luz se transmite por el interior del núcleo mediante una refracción gradual. Esto es debido a que el núcleo se construye con un índice de refracción que va en aumento desde el centro a los extremos. Suele tener el mismo diámetro que las fibras multimodo. Su cubierta suele ser de color naranja.



[Mrzeon. Tipos de fibra \(CC BY-SA\)](#)

La velocidad de transmisión es muy alta, pudiendo llegar hasta 100 Gbps . Además permite que la atenuación sea mínima, con lo que la señal puede transmitirse a longitudes mayores que con cable de par trenzado o coaxial, y no es interferida por ondas electromagnéticas. Sin embargo, su instalación y mantenimiento tiene un coste elevado. Habitualmente se emplea cuando es necesario cubrir largas distancias o la cantidad de información es alta.

Categoría	Ancho de banda modal mínimo	100 Mb Ethernet 100BASE-FX	1 GB (1000 Mb) Ethernet 1000BASE-SX	10 GB Ethernet 10GBASE-SR	40 GB Ethernet	100 GB Ethernet
OM1 (62.5/125)	200 / 500 MHz·km	Hasta 2000 metros (FX)	275 metros (SX)	33 metros (SR) ^I	No soportado	No soportado
OM2 (50/125)	500 / - MHz·km	Hasta 2000 metros (FX)	550 metros (SX)	82 metros (SR) ^I	No soportado	No soportado
OM3 (50/125) Laser Optimized	1500 / 2000 MHz·km	Hasta 2000 metros (FX)	550 metros (SX)	300 metros (SR) ^I	100 metros 330 metros QSFP+ eSR4	100 metros
OM4 (50/125) Laser Optimized	3500 / 4700 MHz·km	Hasta 2000 metros (FX)	1000 metros (SX)	400 metros (SR) ^I	150 metros 550 metros QSFP+ eSR4	150 metros

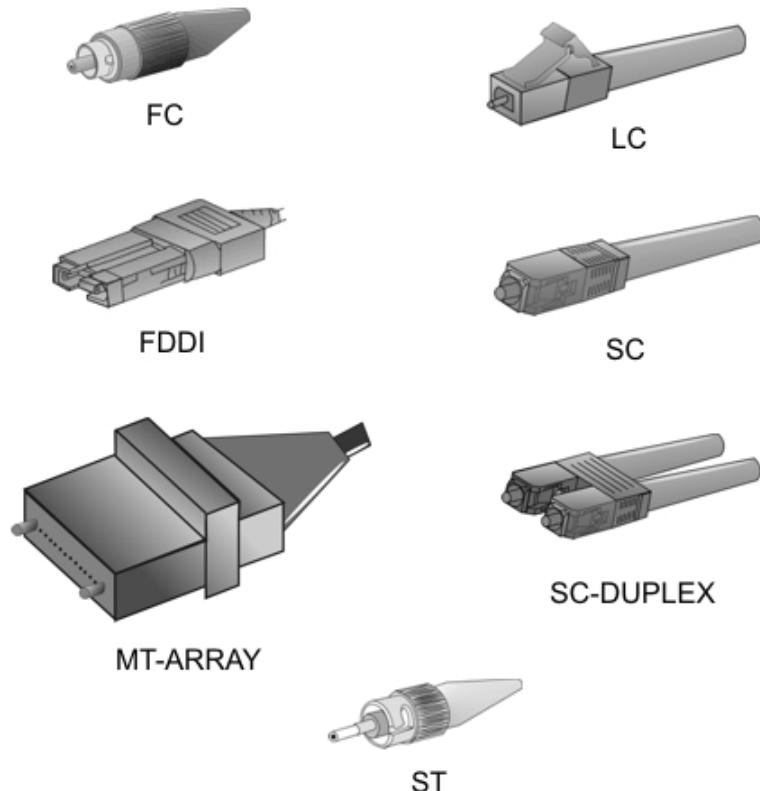
[AlvaroOrellanaGutierrez](#). Tabla Comparativa Fibra Óptica Multi-Modo y Mono-Modo (CC BY-SA)

Los conectores empleados para los cables de fibra óptica son:

SC (Straight Connection): Conector de inserción directa. La conexión de la fibra óptica al conector requiere el pulido de la fibra y la alineación de fibra-conector. Suele utilizarse con fibras monomodo.

ST (Straight Tip): es un conector semejante al SC pero requiere un giro del conector para la inserción del mismo, de modo semejante a los conectores coaxiales. Suele utilizarse en instalaciones Ethernet híbridas entre cables de pares y fibra óptica (fibras multimodo). Como en el caso del conector SC, también se requiere el pulido y la alineación de la fibra.

LC (Lucent conector): un conector pequeño que está adquiriendo popularidad en su uso con fibra monomodo. También admite la fibra multimodo.



[ElSanto510. ULE. Tipos de conectores de fibra \(CC BY-SA\)](#)

La terminación y el empalme del cableado de fibra óptica requieren de equipo y capacitación especiales. La terminación incorrecta de los medios de fibra óptica produce una disminución en las distancias de señalización o una falla total en la transmisión.

Autoevaluación

¿Cuál es la ventaja de utilizar cable de fibra óptica en las redes?

- Su bajo precio.
- Es fácil de instalar.
- No es susceptible a la interferencia electromagnética.
- Se encuentra disponible con o sin blindaje externo.

El precio no es precisamente una ventaja.

No exactamente, hay otras más fáciles y menos costosas.

Correcto. Las interferencias electromagnéticas en la fibra óptica son mínima debido a que circula una señal de naturaleza óptica. Esa ventaja no está presente en los otros medios de transmisión, par trenzado y coaxial, donde el tipo de señal es de naturaleza eléctrica.

NO es correcto, creo que deberías volver a leer el apartado.

Solución

1. Incorrecto
2. Incorrecto
3. Opción correcta
4. Incorrecto

¿Cuáles son las tres clases principales de medios guiados?

- Cables de dos hilos, de 4 hilos y de 8 hilos.
- Par trenzado, coaxial y fibra óptica.
- Infrarojos, ondas de radio, microondas.
- UTP, STP, SFTP.

No son exactamente las clases principales.

Correcto. Los tres principales medios de transmisión cableados utilizados en la implantación de redes de ordenadores son el par trenzado y la fibra óptica. El cable coaxial está perdiendo fuerza en las redes locales aunque se emplea bastante en las redes de cables y en TV.

Vamos mal, pedimos los guiados.

NO, pedimos las principales.

Solución

1. Incorrecto
2. Opción correcta
3. Incorrecto
4. Incorrecto

7.3.- Los estándares y tipos de Ethernet.

Ethernet es una tecnología con múltiples variantes, como otro tipo de tecnologías se pueden clasificar atendiendo al medio de transmisión que utilizan, en este caso al tipo de cable.

La Ethernet se rige por los estándares IEEE 802.3. Actualmente, se definen principalmente cuatro velocidades de datos para el funcionamiento con cables de fibra óptica y de par trenzado:

- 10 Mbps. - Ethernet
- 100 Mbps. - **Fast** Ethernet
- 1000 Mbps. - Gigabit Ethernet
- 10 Gbps. - 10 Gigabit Ethernet

Si bien existe una gran cantidad de implementaciones de Ethernet diferentes para estas diversas velocidades de transmisión de datos (o ancho de banda), tipo de cable, longitud máxima y topología. Aquí sólo se presentarán las más comunes.

TIPO DE ETHERNET	ANCHO DE BANDA	TIPO DE CABLE	LONGITUD MÁXIMA
10Base5	10 Mbps	Coaxial grueso	500 m
10Base2	10 Mbps	Coaxial fino	185 m
10BaseT	10 Mbps	UTP Cat3/Cat5	100 m
100BaseTX	100 Mbps	2 pares STP o UTP Cat5 o mayor	100 m
100BaseFX	100 Mbps	2 Fibras ópticas multimodo	500 m
100BaseT4	100 Mbps	4 pares UTP de Cat 3 a 5	100 m
1000BaseCX	1000 Mbps	4 pares STP Cat 5e o 6	25 m
1000BaseTX	1000 Mbps	4 pares UTP Cat 5e o 6	100 m
1000BaseSX	1000 Mbps	2 fibras ópticas multimodo	550m
1000BaseLX	1000 Mbps	2 fibras ópticas multimodo 2 fibras ópticas monomodo	550 m 2 a 10 km
10GBaseT	10 Gbps	4 pares UTP Cat 6	100 m
10GBaseLX4	10Gbps	2 fibras ópticas monomodo	10 km
10GBaseS	10 Gbps	2 fibras ópticas multimodo	300 m
10GBaseE	10 Gbps	2 fibras ópticas	40 km

Nota aclaratoria: Es posible utilizar de forma indistinta las notaciones Mb/s que Mbps para indicar la velocidad de transferencia.

Veamos las características básicas de algunos de estos estándares Ethernet:

10Base5. Es la especificación original de Ethernet y utiliza coaxial grueso para el transporte de las señales en banda base. También se denomina thick Ethernet.

10Base2. También es una especificación original de Ethernet que utiliza cable coaxial fino, en concreto se suele utilizar el cable RG-58, de 50 ohmios de impedancia, para transmisiones de hasta 10 Mbps. Dichas implementaciones ya no se utilizan y los más recientes estándares 802.3 no las admiten. • **10BaseT.** Utiliza cables de par trenzado UTP para producir transmisiones de hasta 10 Mbps. Configura la Ethernet como una estrella al igual que el resto de los estándares. Permite transmisión full-dúplex para ello utiliza un par de cables para transmitir y otro par para recibir.

100BaseTX. Es semejante al 10 BaseT, pero con velocidades hasta 100 Mbps, utilizando cables UTP de categoría 5. Permite transmisión full-dúplex para ello utiliza un par de cables para transmitir y otro par para recibir.

1000BaseTX. En este caso las comunicaciones siguen la normativa Ethernet pero con velocidades de 1000 Mbps (1 Gbps). Sin embargo se necesitan cables superiores al UTP de categoría 5, por ejemplo, el de categoría 5 mejorado (categoría 5e). Además las distancias de cable deben ser mucho más reducidas. Al contrario de sus primos 10BaseT y 100BaseT, usan los 4 pares de cable de forma paralela tanto para transmitir como para recibir. Es la base de la tecnología Gigabit Ethernet.

1000BaseLX. La velocidad sigue siendo de 1000 Mbps, pero utilizando la fibra óptica como medio de transmisión. Cuando la fibra es multimodo se pueden llegar hasta los 550 m, pero con fibra monomodo se consigue llegar hasta los 2 km y, si la instalación es buena, superar esta distancia hasta llegar a los 10 km.

En algunas instalaciones de alto rendimiento ya se está instalando Ethernet 10G, que sería la red con tecnología Ethernet a 10 Gbps, mayoritariamente sobre fibra, aunque hay algunos intentos con éxito utilizando cableado trenzado de cobre.

* La palabra **Base** quiere decir que son transmisiones en las que no hace falta adaptar la señal al canal, se transmite solo una señal.

Recientemente Cisco ha desarrollado junto con otras compañías la tecnología mGig y estandarizado el 2.5GBASE-T y 5GBASE-T para aprovechar el cableado más común instalado en la mayoría de sitios, (UTP Cat 5e o 6) y sin recablear usar velocidades de 2.5 o 5 Gbps (con UTP Cat 6 hasta 10Gbps) que permitirán dar servicio a los nuevos estándares de WiFi de alta velocidad a la vez que implementa el power over Ethernet según la norma IEEE 802.3at.

Esto permite con un solo cable UTP "común" proveer de alimentación y datos para puntos de acceso Wi-Fi que implementen los estándares de alta velocidad 802.11ac y 802.11ax.

Debes conocer

Es importante saber que hay una equivalencia entre los estándares de capa física y el estándar de capa de subred en TCP/IP correspondiente que la contiene, que es 802.3 en general pero se van haciendo añadidos/revisiones particulares.

Las diferentes normas 802.3 suelen incluir tanto la capa física como la de enlace como ya vimos en la arquitectura TCP/IP. Aunque a veces se habla para distinguir de que 802.3 define los protocolos de capa de enlace y los estándares del tipo 100BaseT definen las normas de capa física.

Por ejemplo:

La norma IEEE 802.3u (**FastEthernet**) define a nivel de capa de enlace el protocolo MAC y CSMA/CD y define tres nuevas capas físicas, que son las siguientes particularizaciones de la más genérica **100Base-T**:

100Base-TX, que requiere dos pares UTP categoría 0 ó dos pares STP categoría 1.

100Base-FX, que utiliza dos fibras multimodo.

100Base-T4, que precisa cuatro pares UTP categoría 3 ó mejor.

Hay una inmensa cantidad de estándares que no ha parado de crecer hasta llegar incluso a los 100Gbps. Puedes encontrar la tabla completa aquí con sus equivalencias de normas de capa física y subred:

https://es.wikipedia.org/wiki/Capa_física_de_Ethernet

Autoevaluación

¿Cuáles de las siguientes opciones son tecnologías Fast Ethernet?

- 100BASE-5.
- 100BASE2.
- 1000BASE-F.
- 100BASE-TX.

No es correcto, esta tecnología basada en cable coaxial opera a 10Mbps (10Base5).

No es correcto, esta tecnología basada en cable coaxial opera a 10Mbps (10Base2).

Incorrecto, esta tecnología se basa en fibra óptica.

Correcto. La tecnología Fast Ethernet opera a 100 Mbps basadas en par trenzado (100BaseTX) y fibra óptica (100BaseF). Las tecnologías 100Base2 y 100Base5 basadas en cable coaxial no operan a velocidades de 100Mbps sino 10Mbps (10Base2 y 10Base 5).

Solución

1. Incorrecto
2. Incorrecto
3. Incorrecto
4. Opción correcta

¿Qué significa la notación 100BASE-TX?

- Velocidad de transmisión de 10 Mbps, banda base y medio físico fibra óptica.
- Velocidad de transmisión de 100 Gbps, banda base y medio físico fibra óptica.

- Velocidad de transmisión de 100 Mbps, banda base y medio físico par trenzado.
- Velocidad de transmisión de 100 Mbps, banda ancha y medio físico fibra óptica.

Incorrecto.

Incorrecto.

Correcto. Cada tecnología Ethernet se expresa por los tres siguientes términos: Velocidad - 100 (100 Mbps), tipo de transmisión - Base (banda base) y medio de transmisión - Tx (par trenzado).

Incorrecto.

Solución

1. Incorrecto
2. Incorrecto
3. Opción correcta
4. Incorrecto

¿Cuál de las siguientes opciones describe lo que es el modo full duplex?

- El tráfico viaja en una dirección a la vez, sin colisiones.
- El tráfico viaja más rápidamente corriente abajo que corriente arriba.
- El tráfico viaja en las dos direcciones a la misma velocidad, sin colisiones.
- El tráfico viaja más rápidamente corriente arriba que corriente abajo.

Incorrecto.

Incorrecto.

Correcto. Full dúplex significa que la información trabaja en ambos sentidos SIMULTÁNEAMENTE. Existe otros modos como son el HALF DÚPLEX donde la información puede viajar en ambas direcciones pero NUNCA simultáneamente (por ejemplo el Walkie-Talkie, la fibra óptica) e incluso el modo SÍMPLEX donde la información viaje solo en una dirección (por ejemplo la señal de TV que siempre viaje una única dirección de los repetidores a los televisores).

Incorrecto.

Solución

1. Incorrecto
2. Incorrecto
3. Opción correcta

4. Incorrecto

7.4.- Estructura de la trama Ethernet.

Los impulsos eléctricos (bits) transmitidos por el medio se ordenan en forma de trama a nivel enlace del modelo OSI, esta trama en el protocolo Ethernet organiza la secuencia de bits como se explica en la siguiente figura.

PREÁMBULO (7 BYTES)	INICIO (1)	DIRECCIÓN DESTINO (2 - 6)	DIRECCIÓN ORIGEN (2 - 6)	LONGITUD DATOS (2)	DATOS (0 - 1500)	RELLENO (0 - 46)	CRC (4)
------------------------	---------------	---------------------------------	--------------------------------	--------------------------	------------------------	---------------------	------------

Preámbulo. Son 7 bytes con el formato 10101010 (negociación de la comunicación).

Inicio. Es un campo de 1 byte compuesto por los bits 10101011, indica que comienza la transmisión.

Dirección de destino. Es un campo que puede ocupar de 2 a 6 bytes con la dirección (MAC) del nodo destinatario de la comunicación.

Dirección de origen. Contiene la dirección MAC de la estación que emitió la trama.

Longitud. Especifica la longitud de los datos transmitidos

Datos. Son los datos a transmitir puede tener hasta 1500 bytes.

Relleno. Se utiliza para conseguir que la trama tenga el tamaño mínimo exigible por la normativa.

CRC. Es un campo de 4 bytes que sirve para el control de errores (Código de Redundancia Cíclica).

[Brivadeneira \(CC BY-SA-4.0\)](#)

Para saber más

Como acabas de ver, la transmisión de mensajes que son transmitidos a través de una red, van siendo empaquetados en diferentes tramas para pasar de una capa a otra. En el siguiente enlace puedes ver los diferentes tipos de tramas Ethernet que podemos encontrar en esa comunicación.

[La Trama Ethernet.](#)

7.5.- Colisiones en Ethernet. Algoritmo de acceso al medio. CSMA.

[Frealsanchez \(CC BY-SA-3.0\)](#)

Cuando Ethernet pone una trama en el bus de la red, esta trama viaja por todo el bus para alcanzar a todas las estaciones que están conectadas a él porque cualquiera de ellas, algunas o todas pueden ser las destinatarias de la información que viaja en lo trama.

Sin embargo, una trama no puede saltar a otra red. Se dice que la trama se circumscribe a su dominio de colisión, es decir, una trama solo puede colisionar con otra dentro de su dominio de colisión pues no puede traspasar esta frontera.

Cuando un nodo necesita transmitir información a otro que está en un **dominio de colisión** distinto necesita acudir a los servicios de otros dispositivos de red intermedios como **switches o routers**. Estos dispositivos **separan los dominios de colisión** y son los encargados de ampliar la red de área local con otros dominios de colisión, cada, uno de los cuales se comporta como una red de área local completa. Frecuentemente a estos dominios de colisión se les denomina **segmentos de red**.

Los protocolos de red que funcionan con direcciones de destino de tipo difusión (broadcast), es decir, con más de un destinatario, pueden producir **tormentas de difusión**, en donde se generan avalanchas de tramas que pueden colapsar la red. En estos casos es muy importante que los dominios de colisión estén perfectamente acotados. Así, si se produce una tormenta de difusión, quedará confinada a ese segmento de red y el problema no afectará a otros segmentos.

El protocolo [**CSMA**](#) surge para solucionar el problema del reparto del canal en las redes Ethernet, se basa en obligar a cada estación a "escuchar el canal" antes de transmitir. Si el canal estuviera ocupado, espera para transmitir, si está libre transmite y si escucha una colisión espera un tiempo y luego transmite.

Hay varios tipos de protocolo [**CSMA**](#):

CSMA 1-persistente.

Transmite con probabilidad 1 al estar el canal desocupado.

Una colisión puede ocurrir cuando dos nodos encuentren el canal libre y comiencen a transmitir con una separación en el tiempo menor que la distancia que les separa.

Es sensible a los retardos de línea.

CSMA no-persistente.

Igual que el anterior, antes de transmitir se escucha al canal.

Si el canal está ocupado espera un tiempo para transmitir, este tiempo está calculado por un algoritmo.

Se diferencia con el 1-persistente en que la estación no está escuchando continuamente a que el canal quede libre para transmitir.

Para poco tráfico se comporta peor que el 1-persistente (es más lento) pero cuando el tráfico es alto reduce el número de colisiones.

CSMA p-persistente.

Se utiliza en canales en los que el uso se limita a franjas de tiempo.

Si el canal está desocupado transmite con probabilidad p y $q=1-p$, retarda la transmisión hasta el próximo intervalo de tiempo.

En caso de que el intervalo de tiempo estuviera ocupado el canal se comporta como si hubiera una colisión, espera un tiempo aleatorio para poder volver a transmitir.

Es más eficiente, en general, que cualquiera de los dos anteriores.

CSMA/CD

Cuando una estación detecta una colisión asegura una transmisión de una fracción mínima del frame, esta fracción se denomina JAM y su objetivo es alertar a las demás estaciones. Entonces espera un tiempo antes de volver a intentar la transmisión.

Al detectar una colisión, las estaciones dejan de transmitir, esperan un tiempo aleatorio y vuelven a transmitir.

Ese tiempo se denomina Backoff y debe ser aleatorio para evitar nuevas colisiones.

CSMA/CD (del inglés Carrier Sense Multiple Access with Collision Detection) o, en español, acceso múltiple con escucha de portadora y detección de colisiones es el estandar usado en Ethernet 802.3 en general. Se basa en que los dispositivos de red escuchan el medio antes de transmitir, es decir, es necesario determinar si el canal y sus recursos se encuentran disponibles para realizar una transmisión.

Esto solo será necesario cuando la red use **hubs** (originalmente era un cable Coaxial equivalente a un hub físico) o un **switch** solamente en sus **puertos "half-duplex"**, puesto que en los **"full-duplex"** se usan 2 pares distintos para envío y recepción de tramas entre los equipos, y por lo tanto no se pueden dar colisiones de ningún tipo.

CSMA/CA (del inglés Carrier Sense Multiple Access with Collision Avoidance) o, en español, **acceso múltiple por detección de portadora y prevención de colisiones**, es un protocolo de control de acceso a redes de bajo nivel que permite que múltiples estaciones utilicen un mismo medio de transmisión. Cada equipo anuncia opcionalmente su intención de transmitir antes de hacerlo para evitar colisiones entre los paquetes de datos (comúnmente en redes inalámbricas, ya que estas no cuentan con un modo práctico para transmitir y recibir simultáneamente). De esta forma, el resto de equipos de la red sabrán cuando hay colisiones y en lugar de transmitir la trama en cuanto el medio está libre, se espera un tiempo aleatorio adicional corto y solamente si, tras ese corto intervalo el medio sigue libre, se procede a la transmisión reduciendo la probabilidad de colisiones en el canal. CSMA/CA es utilizada en canales en los que por su naturaleza no se puede usar CSMA/CD. CSMA/CA se utiliza en 802.11 basada en redes inalámbricas.

[Frealsanchez \(CC BY-SA-3.0\)](#)

Autoevaluación

¿Cuál es una de las características de un dominio de colisión?

- Todos los computadores en un solo medio de acceso compartido.
- Todos los computadores que comparten una sola dirección IP.
- Todos los computadores que comparten una sola dirección MAC.
- Todos los computadores dentro de una WAN.

Correcto. Un dominio de colisión es un segmento físico de una red de computadores donde es posible que los paquetes puedan "colisionar" (interferir) con otros. Estas colisiones se dan particularmente en el protocolo de red Ethernet.

Incorrecto. No se puede compartir la IP.

Incorrecto. La dirección MAC es única.

Incorrecto. Las colisiones se dan principalmente en el protocolo Ethernet.

Solución

1. Opción correcta
2. Incorrecto
3. Incorrecto
4. Incorrecto

¿Qué ocurre en una red Ethernet después de haberse producido una colisión?

- a) Los dispositivos involucrados en la colisión tienen un período de tiempo aleatorio para la retransmisión de la trama dañada.
- b) Los dispositivos involucrados en la colisión lanzan una trama indicando la hora en que cada estación puede comenzar a retransmitir.
- c) Los dispositivos involucrados en la colisión no tienen prioridad para transmitir datos.
- d) El trabajo de transmisión se reinicia una vez que se vuelven a emitir todos los datos.

Correcto. Una vez se produce una colisión, las estaciones u equipos involucrados esperan un tiempo no determinado para volver a mandar la trama.

Incorrecto. No indican la hora.

Incorrecto. De hecho son los que transmiten los datos.

Incorrecto. Sólo se retransmite la trama dañada.

Solución

1. Opción correcta
2. Incorrecto
3. Incorrecto
4. Incorrecto

¿Qué indica la palabra "Base" en 10Base2?

- a) La cantidad de estándares utilizados.
- b) Se utiliza la señalización de banda base.
- c) Sólo se utiliza una porción del medio de transmisión.
- d) Se utiliza la señalización de banda ancha.

Incorrecto. Sólo es un estándar.

Correcto. En Telecomunicaciones, el término banda base se refiere a la banda de frecuencias producida por dispositivo generador de señales (por ejemplo una tarjeta de red) que no es necesario adaptarlo al medio por el que se va a trasmisir. Banda base es la señal de una sola transmisión en un canal, banda

ancha significa que lleva más de una señal y cada una de ellas se transmite en diferentes canales, hasta su número máximo dependiente del canal.

NO va por ahí. Aporta información sobre la transmisión.

Incorrecto. Banda ancha significa que lleva varias señales.

Solución

1. Incorrecto
2. Opción correcta
3. Incorrecto
4. Incorrecto

7.6.- Hub o concentrador.



[Br-278. Hub \(CC BY\)](#)

Un hub, también conocido como concentrador, es un dispositivo de red que actúa como punto de conexión central entre los nodos que componen una red. Los equipos conectados al propio hub son miembros de un mismo segmento de red, y comparten el ancho de banda del hub para sus comunicaciones.

Los hubs aparecieron como solución al problema de las redes que se conectaban a un único cable (redes en bus), ya que si este cable se deterioraba, la red dejaba de ser operativa. El hub hace de punto central de todas las conexiones, de manera que si un cable de conexión de un equipo a la red se estropea, el resto de la red puede seguir operativa. Un hub es el centro donde convergen las conexiones de todos los equipos.

Los hubs pueden ser de dos tipos:

Activos: realizan la regeneración de la señal que reciben antes de ser enviada.

Pasivos: en este caso no regeneran la señal, limitándose a interconectar los equipos.

Su funcionamiento es muy sencillo, todos los equipos de la red se conectan a un núcleo central, el hub, mediante un cable. Cuando un equipo envía un mensaje, los datos llegan al hub y éste los regenera (si es un hub activo) y los retransmite a todos los puestos que estén conectados a cada uno de sus puertos. El uso de hubs crea una topología lógica en bus aunque su topología física es en estrella. Los puertos utilizan un método de ancho de banda compartido y a menudo disminuyen su rendimiento en la LAN debido a las colisiones y a la recuperación frente a éstas. Si bien se pueden interconectar múltiples hubs, éstos permanecen como un único dominio de colisiones.

Los hubs pueden a su vez conectarse entre sí, normalmente por medio de unos puertos especiales denominados in/out o uplink . Existen dos formas posibles de conexión:

En cascada: cada hub conectado al siguiente.

En estrella: cada uno de ellos se conecta a un hub central.

Autoevaluación

¿Cuáles son los puertos que utiliza un hub para enviar el tráfico que recibe en uno de sus puertos?

- Al puerto donde se encuentra el host destino solamente.
- A los puertos en todos los demás dominios de colisión.
- Todos los puertos menos el puerto de origen.
- Todos los puertos.

Incorrecto. No tiene forma de discriminar la salida.

Vamos mal, con eso de varios dominios de colisión.

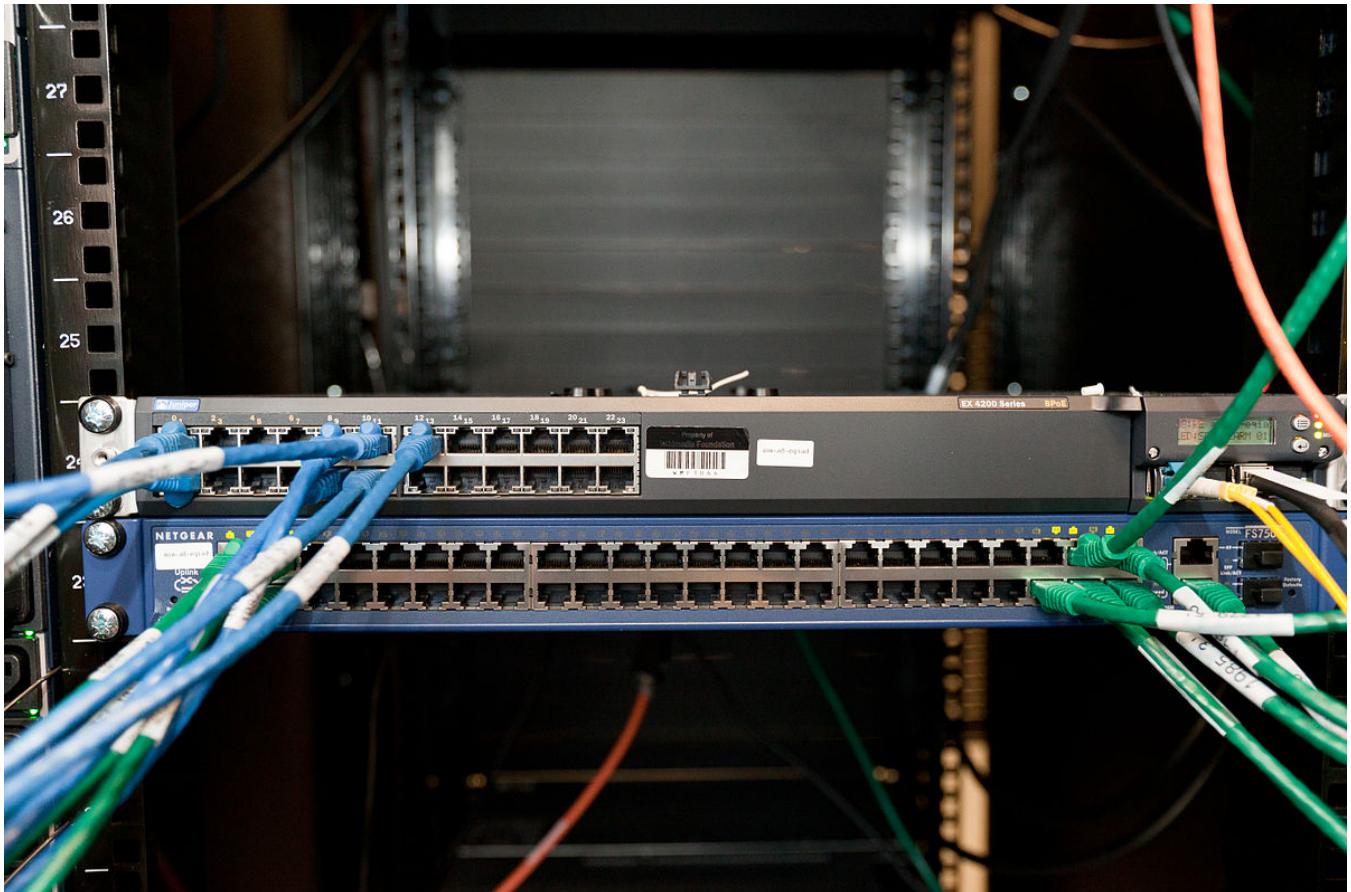
Correcto. Un hub también se conoce como repetidor multipuerto de forma que la trama que le entra por un puerto se retransmite por el resto.

Incorrecto. Casi lo tienes, hay uno por el que no envía.

Solución

1. Incorrecto
2. Incorrecto
3. Opción correcta
4. Incorrecto

7.7.- Switch o conmutador.



[Helpameout, switch \(CC BY-SA\)](#)

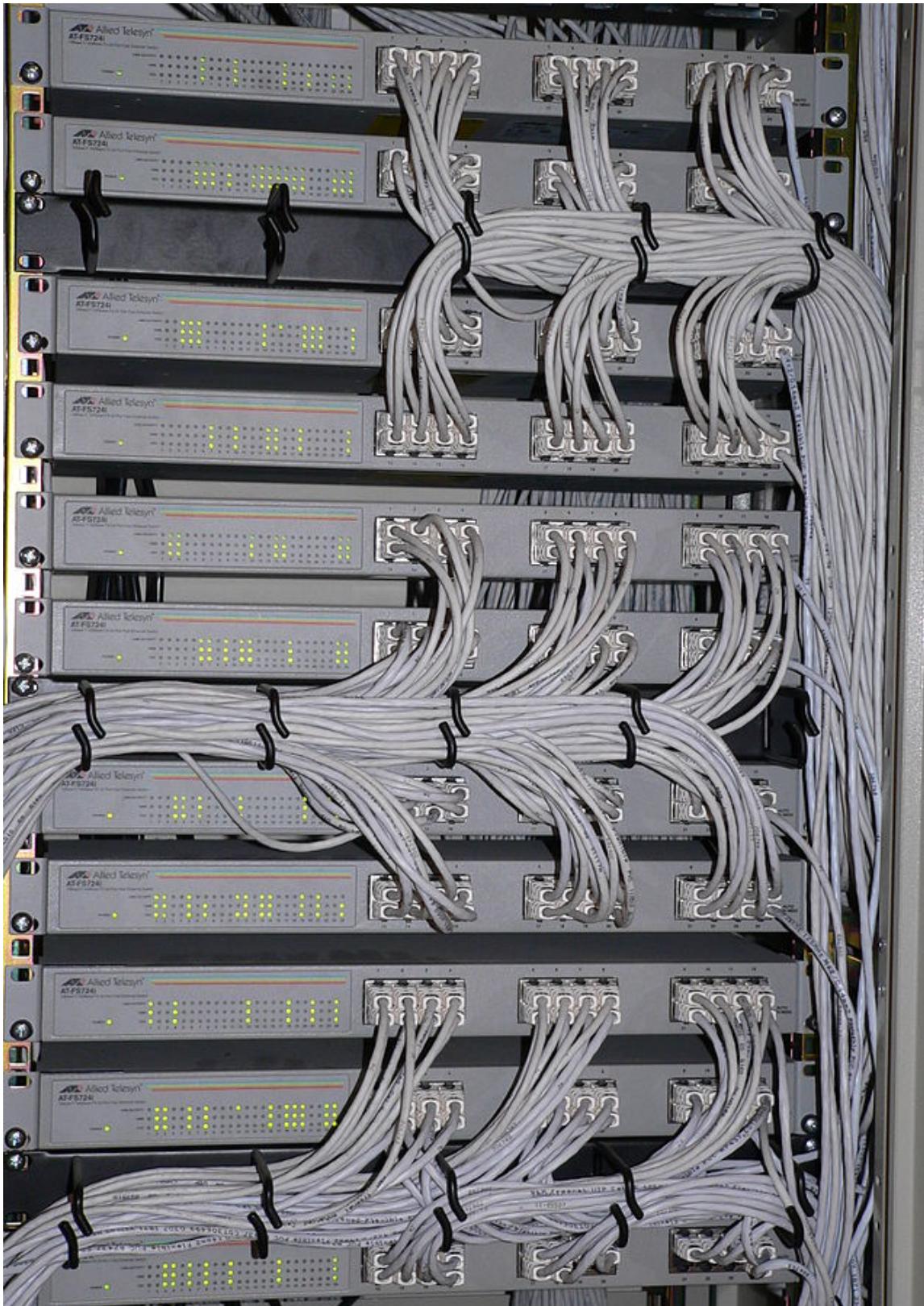
Un switch, también conocido como conmutador, es un dispositivo de red que permite la interconexión de redes de área local a nivel de enlace (capa 2 OSI). Su principal función es segmentar una red en dominios de colisiones (o segmentos de red) para aumentar su rendimiento.

Filtran y dirigen tramas entre los segmentos de la red de área local proporcionando un ancho de banda dedicado y así aumenta el rendimiento de la LAN. Forman un canal de comunicación entre el equipo emisor y el receptor, y disponen de todo el ancho de banda del medio durante la fracción de segundo que tardan en realizar la transmisión (**conexiones punto a punto**).

La función de un switch consiste en tomar la dirección **MAC** de una trama de datos y, en función de ella, enviar la información por el puerto correspondiente. En comparación con el hub, actúa más inteligentemente ya que filtra el tráfico y tiene capacidad de reconocimiento. Los datos pueden conducirse por rutas separadas, mientras que en el hub, las tramas son conducidas por todos los puertos.

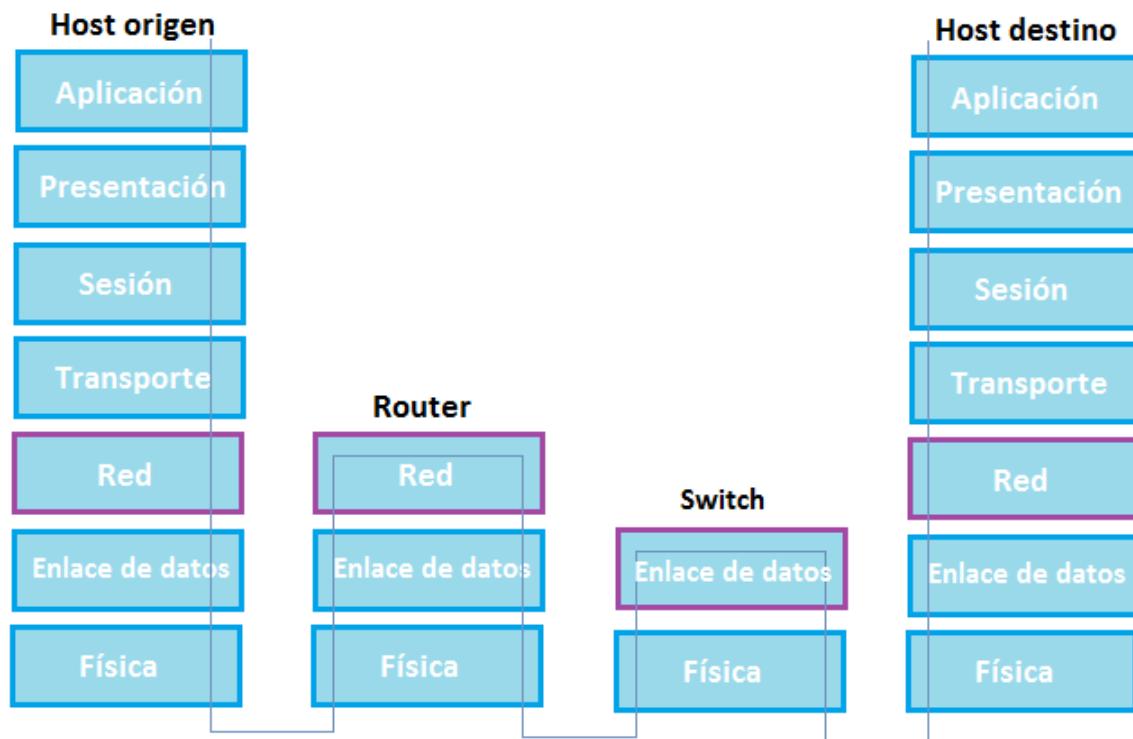
Las redes conmutadas son más rápidas puesto que el ancho de banda perdido por colisiones se elimina. Por ejemplo, si un hub de 24 puertos tiene un dominio de colisión, un conmutador de 24 puertos tendría 24 dominios de colisión.

Evidentemente son algo más complejos de configurar y administrar que los hubs y por supuesto más caros.



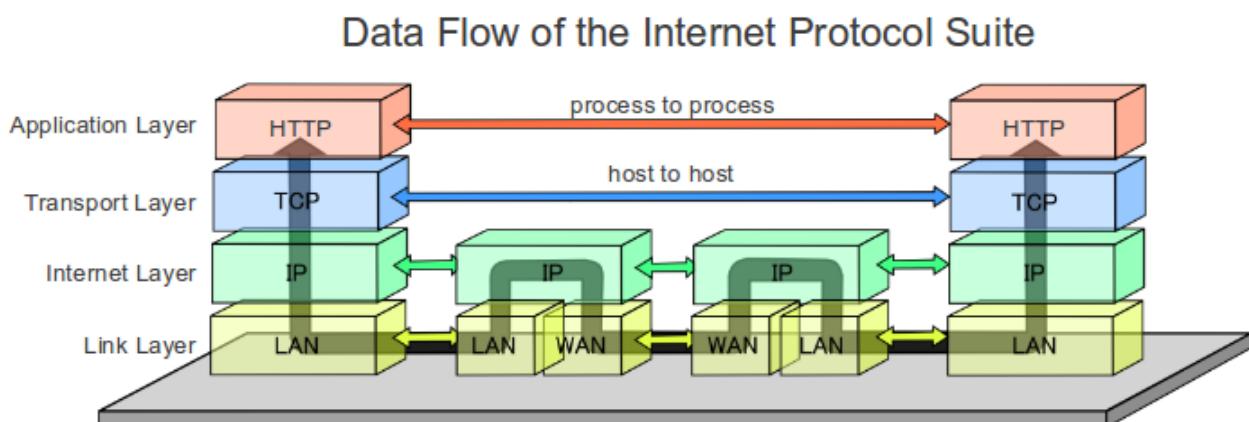
[Parkis, switches en un rack \(CC BY-SA\)](#)

Es importante que tengas en cuenta que los switches (y los hubs también) actúan de manera "transparente" y "plug&play", sin alterar las tramas, no tocan la MAC de origen ni la de destino que las pondrá el equipo emisor. Los switches se dice que trabajan a nivel de capa 2 porque en función de la dirección MAC de destino enviarán la trama por el interfaz o puerto correspondiente según su tabla de MACs que haya ido aprendiendo mientras escuchan los ARP's y todas las comunicaciones que pasan por ellos, fijándose en la MAC de origen de las tramas que entran por cada uno de sus puertos.



[xrespo11. Capas OSI en hosts, switches y routers \(CC BY-SA\)](#)

Los **routers o encaminadores** se verán en detalle en posteriores unidades, pero debes saber que serán los encargados de encaminar los paquetes a nivel de capa 3 o de red, en función de su tabla de rutas. También veremos más en detalle en próximas unidades como los routers serán "transparentes" a nivel de capa 3 (no alterarán salvo que hagan NAT las IPs de origen y destino), pero sí que alterarán las MAC de origen y destino en cada salto de red. En la siguiente imagen se puede ver una imagen que mezcla varios conceptos, por ejemplo LAN y WAN no son protocolos, pero está bien para conceptualizar como se encapsula cuando tenemos 2 PCs comunicándose a través de 2 routers que están conectados por una conexión WAN.



[Rob-norman. Torre de protocolos entre 2 PCs conectados por 2 routers \(CC BY-SA\)](#)

Autoevaluación

¿Qué dispositivos de nivel 2 permite segmentar la red?

- Repetidor.
- Switch o conmutador.

- Concentrador o Hub.
- Enrutador o router.

Incorrecto. No permite segmentar.

Correcto. El switch es un dispositivo de nivel 2 (trabaja hasta la capa 2) que permite establecer dominio de colisión (segmentar la red).

Incorrecto. En él convergen todas las conexiones.

Incorrecto. Pregunta por el nivel 2.

Solución

1. Incorrecto
2. Opción correcta
3. Incorrecto
4. Incorrecto

7.8.- Película "Warriors of the Net"

Un recurso de entretenimiento para ayudar a visualizar los conceptos de redes es la película animada "**Warriors of the Net**" (Guerreros de la red), por TNG Media Lab.

Antes de ver el video, te aviso que es un vídeo antiguo y con algunos errores técnicos de concepto, además debes tener en cuenta lo siguiente:

Primero, en cuanto a los conceptos que has aprendido hasta ahora, piensa en qué momento del video está en la LAN, en la WAN, en la **intranet** (un conjunto de webs o servicios solo accesibles desde la LAN de la empresa que también se le puede referir como intranet) o en Internet, y cuáles son los dispositivos finales vs. los dispositivos intermedios, cómo se aplican los modelos OSI y TCP/IP y qué protocolos están involucrados.

Segundo, es posible que algunos términos que se mencionan en el video no te sean familiares. Los tipos de paquetes mencionados se refieren al tipo de datos de nivel superior (TCP, UDP, ICMP Ping, PING de la muerte) que se encapsulan en los paquetes IP (en definitiva, todo se convierte en paquetes IP). Los dispositivos o conceptos que encuentran los paquetes en su viaje son router, servidor proxy, router-switch, Intranet corporativa, el proxy, la URL (Localizador universal de recursos) del navegador de Internet, el firewall, el ancho de banda del canal de comunicaciones, un host u ordenador con conexión a Internet, un servidor Web, etc.

Tercero, mientras que en el video se hace referencia explícita a los puertos (TCP o UDP) con números 21, 23, 25, 53 y 80, solamente se hace referencia implícita a las direcciones IP. ¿Puedes ver dónde? ¿Dónde se muestra en el video que las direcciones MAC pueden estar involucradas?

Seguramente encuentras algunos términos que aún no conoces, no te preocupes, a lo largo del ciclo los irás conociendo y está bien que te vaya resultando familiar.

Otros errores de conceptos a tener en cuenta:

Las colisiones antes eran muy comunes en la LAN porque en vez de switches (conmutadores) se usaban hubs (concentradores) donde todos los equipos compartían el mismo medio. Por eso hay tantas colisiones, pero a día de hoy no hay porque se usan switches con "almacenamiento y reenvío" (store and forward) con ancho de banda dedicado para cada uno de sus interfaces. Y en WiFi, aunque sí haya medio compartido, se usa CSMA/CA para "evitar" las colisiones mediante un sistema de slots de tiempo para transmitir cada estación regulado por el Access Point.

El concepto de "etiqueta para el proxy" no es correcto del todo. Entender como funciona un proxy es complejo y hay varios tipos. Existen en general 2 tipos de proxys, el transparente y el no transparente.

Normalmente en una red hay varios firewall (cortafuegos) localizados en varios sitios, además de tener programas de firewall-antivirus en los PCs y funcionalidad de firewall en los routers. Lo más común es que el punto más exterior de la empresa sea el router con una conexión WAN de algún tipo, pero con funcionalidad de firewall interna. Y si se tiene un equipo adicional de firewall más avanzado/potente, se coloca tras el router.

Aquí no se habla nada de NAT, pero es de lo más común encontrarlo a la salida de todos los routers, y de paso es un punto de protección a la entrada. Al principio de Internet no era tan común usar NAT porque no había problemas de escasez de direcciones IP públicas.

Puedes descargar la película de <http://www.warriorsofthe.net> o visionarla en español a través de los siguientes enlaces:

[1^a Parte](#)

[2^a Parte](#)

[Vídeo completo con algunas explicaciones extra](#)

Resumen del video WARRIORS OF THE.NET:

Todo empieza cuando se quiere mandar un paquete, para eso se necesita ponerle una dirección (IP) que va a ir dirigido a Internet. Ésta recibe una etiqueta del servidor Proxy y en ese momento salen de nuestra maquina y se dirigen por la red cableada y es lanzado hacia la red de área local o LAN que es usada para conectar todas la computadoras locales.

La LAN no es un lugar muy confiable y pueden surgir accidentes, el Router local lee las direcciones y si es necesario pone los paquetes en otra red, no es muy rápido pero casi siempre es exacto, cuando dejan el router siguen su camino por la red, cuando los paquetes llegan a su destinos son interceptados por la interfaz de red para ser enviados al siguiente nivel Proxy que sirve para establecer y compartir entre varios usuarios una conexión y también por seguridad.

El proxy busca la dirección URL y si está permitida la manda a Internet. El proxy se puede configurar para permitir solo algunas direcciones.

Luego el paquete vuelve a la ruta por el LAN y después sigue el Firewall que previene intermisiones provenientes de Internet y para que la información confidencial no sea enviada.

Después llega a Internet, una telaraña de redes que se enlaza a través de Satélites, líneas telefónicas o incluso a través del mar.

Cerca del fin del viaje donde se localiza la dirección solicitada, después llega al Firewall de entrada en la red de destino, y está diseñado solo para dejar entrar a los paquetes que cumplen con un criterio de selección, y solo tiene algunos puertos abiertos disponibles de algunos servicios de red concretos.

Casi a punto de terminar siguen los paquetes por la interfaz de red de la LAN de destino para llegar a un servidor web, se reciben los paquetes abiertos y desempaquetados, la información que contiene es enviada hacia la aplicación del servidor web.

Por ultimo el paquete se recicla para continuar de nuevo y seguir el mismo camino de vuelta. Es decir, se intercambian las IPs de destino y origen para devolver al cliente web la información de la página web pedida en otros paquetes IP.

Recomendación

Puedes practicar tratando de resolver las siguientes ACTIVIDADES:

- Haz un diagrama de red y un esquema de todo el trayecto que realiza el paquete de la peli. Usa números para ir indicando el orden de los sucesos.
- Nombra y define cada uno de los equipos de red que aparecen en la peli.
- Nombra y define cada uno de los tipos de paquetes que aparecen en la peli.
- ¿Qué diferencia existe entre un proxy y un firewall?
- ¿Cuales son los puertos que normalmente tiene abiertos el firewall de un servidor web y para qué sirven cada uno?
- ¿Cómo se envían los paquetes por la red? ¿Qué significa el concepto de encapsulamiento?

8.- Planificación de Redes.

Caso práctico

En los apartados anteriores hemos estudiado distintas medios de transmisión y tecnologías de redes que podemos implementar. Antes de proceder a la instalación física de nuestra red tenemos que realizar un estudio previo que recoja todas las necesidades, factores de costo y opciones de implementación de nuestra academia. . Se debe planificar y diseñar nuestra red.

Estas necesidades se tienen que recoger de una manera formal en una serie de documentos donde se recoja una propuesta de diseño de nuestra red, costes, opciones y las fases de elaboración del mismo. Durante el proceso de planificación se tienen que tomar decisiones en base a una serie de aspectos que veremos a continuación.

Para que una red local (LAN) sea efectiva y pueda satisfacer las necesidades de los usuarios, se debe implementar siguiendo una serie sistemática de pasos planificados.

El **primer paso** en el proceso es reunir información acerca de la organización. Esta información debe incluir:

- 1.- Historia de la organización y situación actual.
- 2.- Crecimiento proyectado.
- 3.- Políticas de operación y procedimientos administrativos.
- 4.- Sistemas y procedimientos de oficinas.
- 5.- Opiniones del personal que utilizará la LAN.

Es de esperarse que este paso también lo ayude a identificar y definir cualquier cuestión o problema que deba tratarse (por ej., puede encontrar alguna sala alejada en el edificio que no tenga acceso a la red).

El **segundo paso** es realizar un análisis y evaluación detallados de los requisitos actuales y proyectados de las personas que usarán la red.

El **tercer paso** es identificar los recursos y limitaciones de la organización. Los recursos de organización que pueden afectar a la implementación de un nuevo sistema LAN se dividen en dos categorías principales: hardware informático/recursos de software, y recursos humanos. Es necesario documentar cuál es el hardware y software existentes de la organización, y definir las necesidades proyectadas de hardware y software. Las respuestas a algunas de estas preguntas también le ayudarán a determinar cuánta capacitación se necesita y cuántas personas se necesitarán para soportar la LAN. Entre las preguntas que realice deberán figurar las siguientes:

- 1.- ¿Cuáles son los recursos financieros disponibles de la organización?
- 2.- ¿De qué manera se relacionan y comparten actualmente estos recursos?
- 3.- ¿Cuántas personas usarán la red?
- 4.- ¿Cuáles son los niveles de conocimiento sobre informática de los usuarios de red?
- 5.- ¿Cuáles son sus actitudes con respecto a los computadores y las aplicaciones informáticas?

A partir de la planificación y diseño de la red se genera algunas de los siguientes documentos:

- Diario de ingeniería (cronograma de actividades).
- Topología lógica.
- Topología física.
- Plan de distribución.
- Matrices de solución de problemas.
- Tomas rotuladas.

Tendidos de cable rotulados.

Resumen del tendido de cables y tomas.

Resumen de dispositivos, direcciones MAC y direcciones IP.

La parte más importante del proceso de diseño de red sea el diseño, de acuerdo con los **estándares industriales de ANSI/EIA/TIA e ISO/IEC**.

Para llevar a cabo el diseño, tenemos que tener en cuenta algunos aspectos que describimos en los siguientes apartados.

8.1.- Cableado estructurado.

El concepto de "cableado estructurado" se entiende como el sistema de cables, conexiones, canalizaciones, espacios y demás dispositivos que deben ser instalados para establecer una infraestructura de telecomunicaciones genérica en un edificio.

La instalación de todos los elementos debe seguir los siguientes estándares para que se califique de cableado estructurado:

- ANSI/TIA/EIA-568-B: Cableado de telecomunicaciones. (cómo instalar el cableado)
- ANSI/TIA/EIA-569-A: Normas de recorridos y espacios de telecomunicaciones. (cómo enrutar el cableado).
- ANSI/TIA/EIA-607: Requerimientos para instalaciones de sistemas de puesta a tierra de telecomunicaciones.
- ANSI/TIA/EIA-570-A: Normas de infraestructura residencias de telecomunicaciones.
- ISO/IEC 11801.

El que la instalación siga un estándar implicará un beneficio en su administración y gestión. Básicamente, el cableado estructurado consiste en el tendido de cables en el interior de un edificio con el propósito de implantar una red de área local.

Partiendo del subsistema de más bajo nivel jerárquico tenemos la siguiente organización:

- Áreas o zona de trabajo o localización de cada puesto de trabajo
- Subsistema o cableado distribuidor o armario (de planta o de edificio).
- Subsistema o cableado horizontal o de planta
- Subsistema o cableado vertical, dorsal (*backbone*) o de edificio.
- Cuarto de telecomunicaciones, entrada de servicios y equipos

Cableado estructurado en un edificio:

- 1.- Cableado de área de trabajo.
- 2.- Cableado horizontal.
- 3.- Cableado de administración (armario de cableado, *rack*).
- 4.- Cableado vertical (central, *backbone*).
- 5.- Centro de cálculo.
- 6.- Cableado de equipamiento (armario de entrada al edificio).
- 7.- Cableado del campus (acometida, cableado entre edificios).

[PePeEfe - Wikipedia \(CC BY-SA\)](#)

Los cambios que se deben realizar en las instalaciones de red, especialmente en su cableado, son frecuentes debido a la evolución de los equipos y a las necesidades de los usuarios de la red. Esto nos lleva a tener en cuenta otro factor importante: la flexibilidad.

Un sistema de cableado bien diseñado debe tener al menos estas dos cualidades: **seguridad y flexibilidad**. A estos parámetros se le pueden añadir otros, menos exigentes desde el punto de vista del diseño de la red, como son el **coste económico**, la **facilidad de instalación**, etc.

La estructuración del cable se consigue construyendo módulos independientes que segmenten la red completa en subsistemas de red, independientes pero integrados, de forma que un subsistema queda

limitado por el siguiente subsistema. Estos subsistemas siguen una organización jerarquizada por niveles desde el sistema principal hasta el último de los subsistemas.

Podemos concluir que el cableado estructurado es una técnica que permite cambiar, identificar, mover periféricos o equipos de una red con flexibilidad y sencillez. Según esta definición, una solución de cableado estructurado debe tener dos características: **modularidad**, que sirve para construir arquitecturas de red de mayor tamaño sin incrementar la complejidad del sistema, y **flexibilidad** que permite el crecimiento no traumático de la red.

El esquema teórico del cableado estructurado sería el siguiente:

Alfonso Bonillo-Elab.Propia (Dominio público)

Alfonso Bonillo-Elab.Propia (Dominio público)

Cableado y equipamiento del área de trabajo

El cableado y equipamiento del área de trabajo no es parte del sistema de cableado genérico y la norma no impone requisitos al respecto. Incluye:

- 1.- Cable del área de trabajo.
- 2.- Equipamiento terminal.

Se asume una longitud eléctrica combinada de (1) y (2) equivalente a 7,5 m de cable.

Distribuciones

Debería haber un mínimo de un armario distribuidor de planta (FD) por cada 1.000 m² de espacio reservado para oficinas, con un mínimo de un FD por planta. Si una planta se utiliza poco para oficinas (como un vestíbulo) puede atenderse desde un FD de una planta adyacente.

Todo distribuidor; de Campus (CD), de Edificio (BD) o de planta (FD), debe estar en un cuarto de telecomunicaciones o en un cuarto de equipamiento.

Todas las interconexiones del cableado genérico se realizan con paneles de conexión.

Cuando los equipos activos (enrutadores, commutadores...) se cablean directamente a paneles de algún subsistema de cableado, se denomina 'interconexión' (interconnect), y cuando lo hacen a paneles independientes se denomina 'conexión cruzada' (cross connect).

Suele ser más eficiente, por coste inicial y de mantenimiento, disponer de pocos distribuidores grandes que de muchos distribuidores pequeños, teniendo en cuenta que la distancia de los FD (Distribuidor de planta) a las TO (toma de usuario) no debe superar los 90 m. Es decir, normalmente, las TO estarán en un radio de 60 m desde el FD, debido a que el cable debe subir, bajar y hacer curvas.

Ademas los FD deben situarse, siempre que haya espacio disponible, lo mas cerca posible de la(s) vertical(es).

En la instalación de los distribuidores de edificio (BD) y de campus (CD) debe considerarse también su proximidad a los cables de comunicaciones con el exterior.

Cuartos de telecomunicaciones/Cuartos de Equipamiento

Un cuarto de telecomunicaciones (TC: Telecommunications Closet) es un espacio cerrado de un edificio utilizado para el uso exclusivo de cableado de telecomunicaciones y sistemas auxiliares: bastidores (racks), concentradores, aire acondicionado propio...Cada cuarto debe tener acceso directo al cable espinazo.

Un cuarto de equipamiento (ER: Equipment Room) es un espacio cerrado de uso específico para equipamiento de datos y telecomunicaciones que puede contener o no distribuidores (haciendo la función de TC). Todo espacio que contenga más de un distribuidor se considera un ER.

Los cuartos de telecomunicaciones deben considerar, además de voz y datos, la incorporación de otros sistemas de información del edificio tales como televisión por cable (CATV), alarmas, seguridad o audio. No debe contener otras instalaciones eléctricas que no sean del equipamiento propio del cuarto.

Un cuarto de equipamiento puede incluir espacio de trabajo para el personal correspondiente.

Los armarios (bastidores o racks) deben de contar con al menos 82 cm de espacio libre por delante y detrás, medidos a partir de la superficie más sobresaliente del armario.

Deben disponer de acometida eléctrica diferenciada, apantallamiento frente a interferencias electromagnéticas, sistemas de alimentación interrumpida, sistema de luz de emergencia y ventilación adecuada.

Todo edificio debe contener al menos un cuarto de telecomunicaciones o un cuarto de equipo; no hay un límite máximo.

En los TC la temperatura debe mantenerse permanentemente entre 10 y 35 grados centígrados y la humedad relativa debe mantenerse por debajo del 85%, realizándose un cambio completo de aire por hora.

En los ER la temperatura debe mantenerse permanentemente entre 18 y 24 grados centígrados y la humedad relativa debe mantenerse entre el 30% y el 55%, realizándose un cambio completo de aire por hora.

Por esto a veces los TC y ER son también llamados "salas frías".

Salidas de Telecomunicacion y Puntos de Transmisión

Una alta densidad de TOs aporta flexibilidad al cableado para permitir cambios. En muchos países se utilizan dos TOs para un máximo de 10m².

Pueden presentarse individualmente, por parejas o en grupo, pero cada área de trabajo debe cubrirse con al menos dos.

Cada TO debe estar identificado con una etiqueta permanente y visible. Si uno de ellos está conectado con cable de par trenzado y utiliza menos de 4 pares debe ser claramente marcado. La configuración mínima consiste en:

Un TO con cable balanceado de 100 Ω, preferentemente cable de 4 pares, categoría 3 o superior.

Otro(s) TO con dos hilos de fibra óptica multi-modo o cable balanceado categoría 3 o superior).

Se conocen como MUTO (Multi-User TO) las rosetas multi-usuario, que pueden dar servicio a 12 áreas de trabajo como máximo (24 TOs). Deben ser fácilmente accesibles y su instalación debe ser permanente, es decir, no pueden estar localizadas en un techo o piso falso, en un armario... El cable desde el FD hasta un punto de transición (TP) o un MUTO debe tener mínimo 15 m.

Un punto de transición (TP) sirve para cambiar entre distintas formas del mismo tipo de cable (p.e. de cable plano a cable redondo) o como punto de consolidación. No puede ser utilizado como

distribuidor ni se pueden conectar a él equipos activos. Las características de los cables deben ser mantenidas en la entrada y la salida.

Los puntos de consolidación son una interconexión en el cableado horizontal que permite configuraciones más sencillas en oficinas cambiantes y se permiten para un máximo de 12 áreas de trabajo (24 TOs).

La diferencia más visible entre un TP y una MUTO es que el TP requiere una conexión adicional (una TO) para cada cable horizontal. Las TP se utilizan en oficinas cambiantes donde las TO se irán moviendo de un sitio a otro y las MUTO en oficinas que necesitan concentrar sus TO.

Tipo de cableado

Los tipos de cable permitidos por la norma vigente son:

Cable de pares trenzados con o sin blindaje de 100 Ω.

Cable de fibra óptica multimodo de 62.5/125 μm.

Cable de fibra óptica multimodo de 50/125 μm.

Cable de fibra óptica monomodo 8-10/125 μm (para largas distancias).

Se usarán preferentemente los dos primeros tipos de cable.

Administración

La administración es un aspecto esencial del cableado genérico. La administración incluye la identificación exacta y el registro de todos los componentes del sistema, así como las canalizaciones y los espacios (TC y ER). Un buen registro puede incluir diagramas de cableado, mapas de conectividad y localización de los TO.

Deben registrarse todos los cambios que se realicen y cuando se han realizado, preferentemente por ordenador, y preparar procedimientos adecuados de actualización.

Si se realizan test de aceptación deberían registrarse también sus resultados.

Cada elemento, canalización y espacio debe tener su identificación claramente visible. A cada elemento, canalización y espacio se le asignará una identificación (mediante colores, números o cadenas alfanuméricas) unívoca.

Cada TO debe etiquetarse de modo que refiera la impedancia del cable, su categoría y número de pares o bien el diseño de fibra óptica utilizado.

Los cables deben marcarse en ambos extremos.

Autoevaluación

Según la normativa, los armarios (bastidores o racks) deben de contar con al menos 82 cm de espacio libre por delante y detrás, medidos a partir de la superficie más sobresaliente del armario.

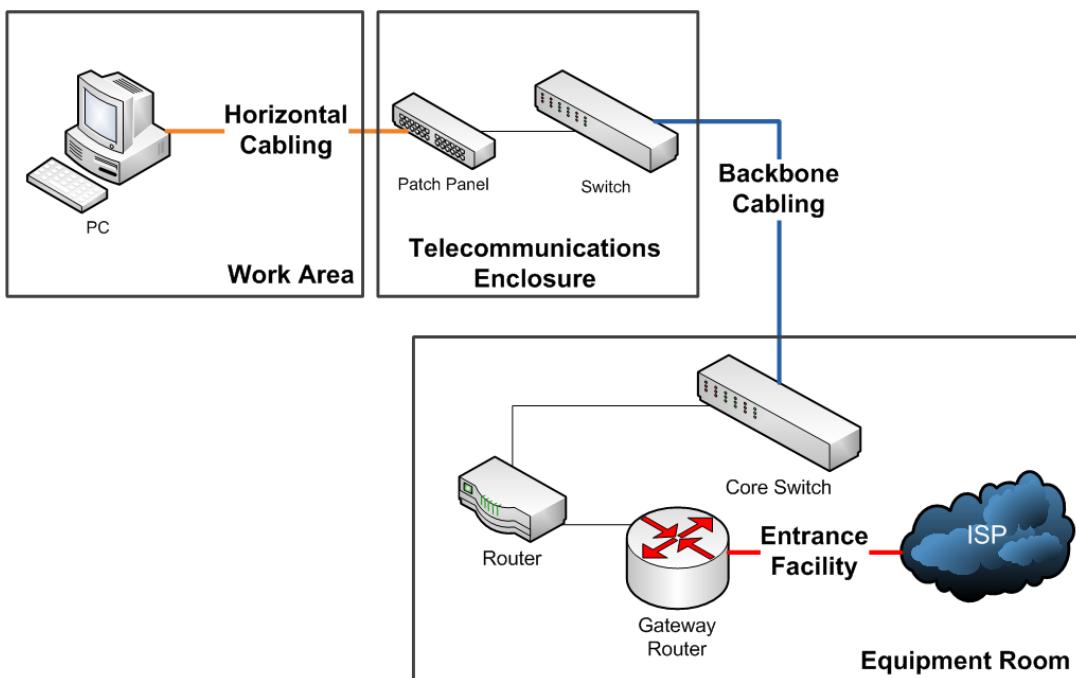
Verdadero Falso

Verdadero

8.1.1.- Áreas de Trabajo o Localización de cada Puesto de Trabajo.

Las áreas de trabajo son las ubicaciones destinadas para los dispositivos finales (por ejemplo PCs) utilizados por los usuarios individuales.

Cada área de trabajo tiene una o dos tomas de usuario que pueden utilizarse para conectar un dispositivo individual a la red. Utilizamos latiguillos (patch cords o patch cables) para conectar dichos dispositivos a estas tomas de red. El estándar EIA/TIA establece que los latiguillos de UTP tienen una longitud máxima de 10 metros. El cable de conexión directa (paralelo) es el latiguillo de uso más común en el área de trabajo.

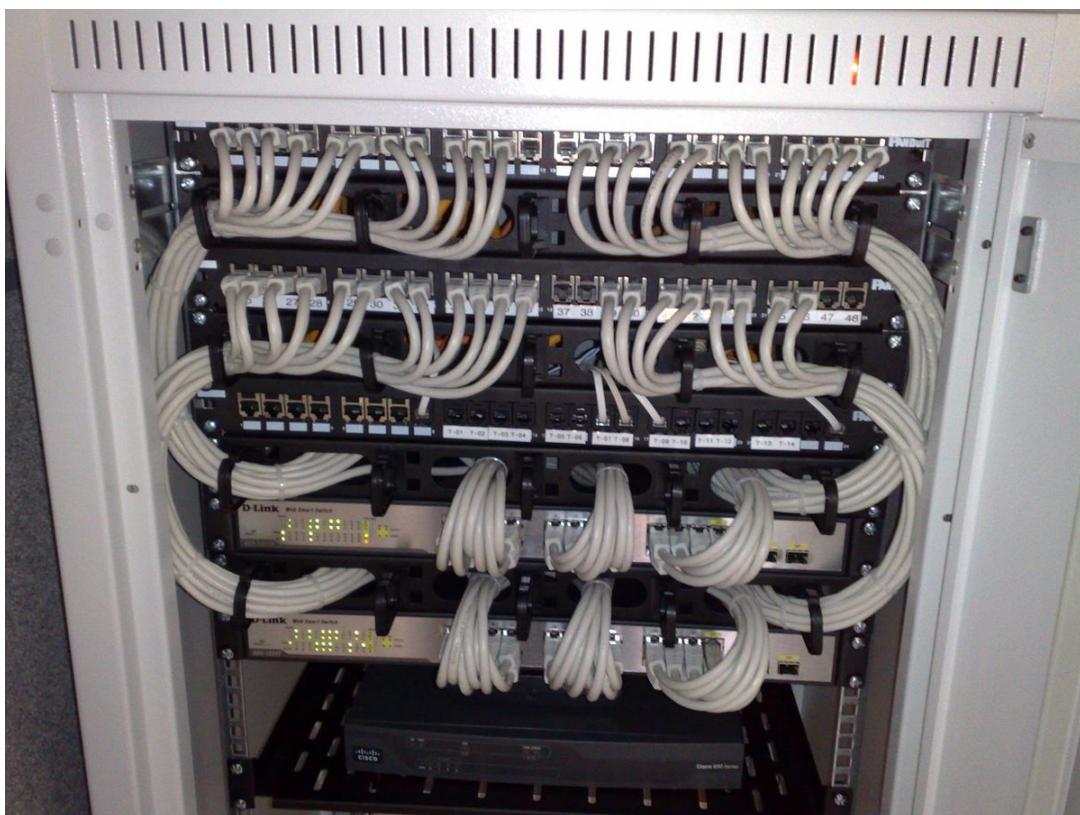


[Lanil Marasinghe \(CC BY-SA\)](#)

8.1.2.- Subsistema Distribuidor o Administrador.

Es el lugar donde se realizan las conexiones del sistema de cableado a los dispositivos de red (hubs, switches, routers, etc). Está formado por racks (armarios distribuidores o repartidores), enchufes, paneles de parcheo (patch pannels), dispositivos de red, servidores, SAI (Sistema de alimentación ininterrumpida), etc.

Normalmente, al igual que en las áreas de trabajo, se emplean latiguillos para conectar los paneles de parcheo y los dispositivos de red.

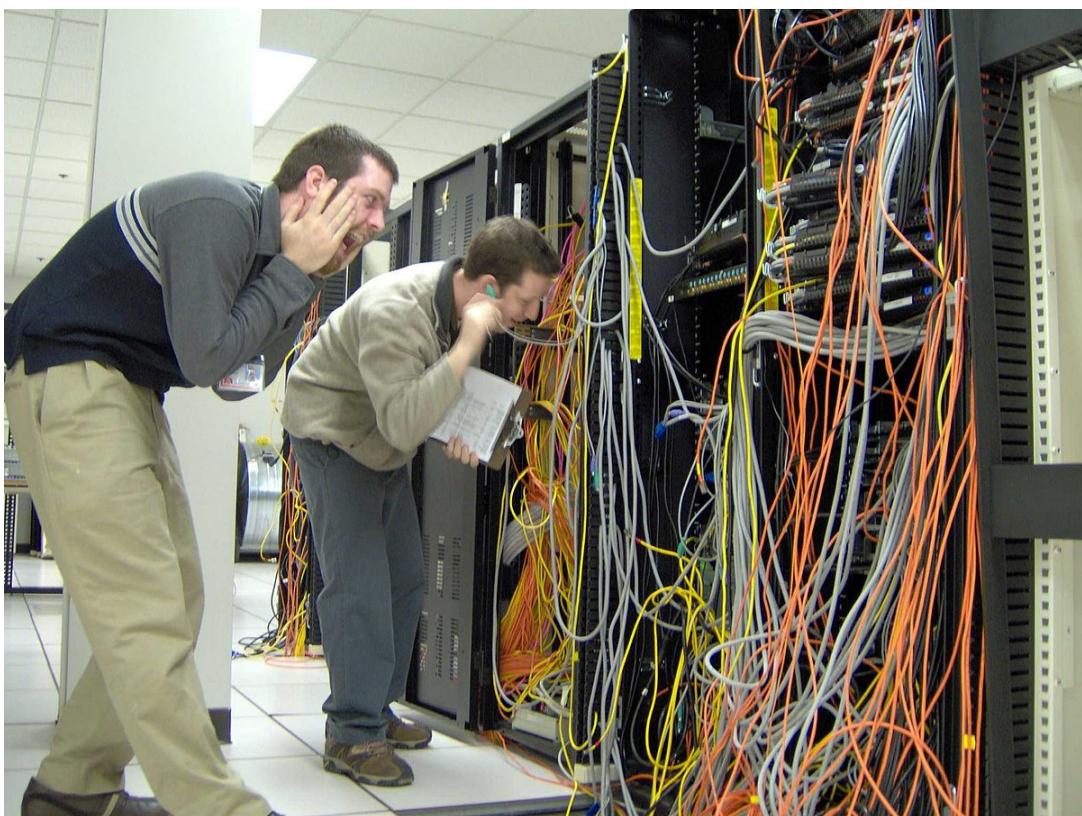


Dsimic ([CC BY-SA](#))

8.1.3.- Cuartos de Telecomunicaciones.

Son las áreas de un edificio para el uso exclusivo de los equipos asociados con el sistema de cableado de telecomunicaciones (voz y datos). Debe ser capaz de albergar equipos de telecomunicaciones, terminaciones de cable y cableado de interconexión asociado.

En el caso de que sea lugar para recoger las entradas de los servicios externos a la organización (líneas telefónicas, accesos a Internet, recepción de TV por cable o satélite...) se le suele denominar cuarto de entrada de servicios.



Clemente (CC BY-SA)

Autoevaluación

A los cuartos de telecomunicaciones que recogen las entradas de los servicios externos a la organización (líneas telefónicas, accesos a Internet, recepción de TV por cable o satélite...) se les suele denominar cuartos de entrada de servicios

- Verdadero Falso

Verdadero

8.1.4.- Subsistema Horizontal o de Planta.

El subsistema horizontal se refiere al sistema de cableado que conecta los subsistemas administradores con las áreas de trabajo. La longitud máxima de cable desde el punto de terminación en el subsistema administrador hasta la terminación en la toma del área de trabajo no puede superar los 90 metros. Los medios horizontales se ejecutan desde el panel de parcheo en el subsistema administrador a una toma de red (roseta) en cada área de trabajo. Las conexiones a los dispositivos de red se realizan con latiguillos.

Los estándares de la Asociación de Industrias Electrónicas y la Asociación de las Industrias de las Telecomunicaciones (EIA/TIA) establecen dos tipos diferentes de latiguillos de UTP. Uno de los tipos es el latiguillo que se utiliza para interconectar el dispositivo de red (hub, switch, etc) y los paneles de parcheo ubicados en el rack (armario de comunicaciones). Otro tipo de latiguillo se utiliza para conectar dispositivos finales a las rosetas. La suma de ambos latiguillos no debe superar los 10 metros.

Alfonso Bonillo-Elab.Propia (Dominio público)

8.1.5.- Subsistema Vertical o Backbone.

El subsistema vertical se refiere al sistema de cableado utilizado para conectar los subsistemas horizontales. También se utiliza para el tráfico de entrada o de salida de Internet, y para el acceso a los recursos corporativos en una ubicación remota. Gran parte del tráfico desde varias áreas de trabajo utilizará el backbone para acceder a los recursos externos del área o la instalación. Por lo tanto, los backbones generalmente requieren de medios de ancho de banda superiores como el cableado de fibra óptica.

[Kecko \(CC BY\)](#)

Autoevaluación

¿El diagrama esquemático de un sistema de cableado estructurado se compone de los siguientes subsistemas de cableado?

- Campus, vertical, horizontal y de zona de trabajo.
- Distribuidor de edificio, de planta, latiguillo y roseta.
- Bajo el suelo, de falso techo y de pared.
- Frontal, lateral, transversal y dorsal.

Correcto. Los subsistemas que forman parte de un cableado estructurado son de nivel mas alto de jerarquía a mas bajo: campus, vertical, horizontal y área de trabajo.

No es correcto.

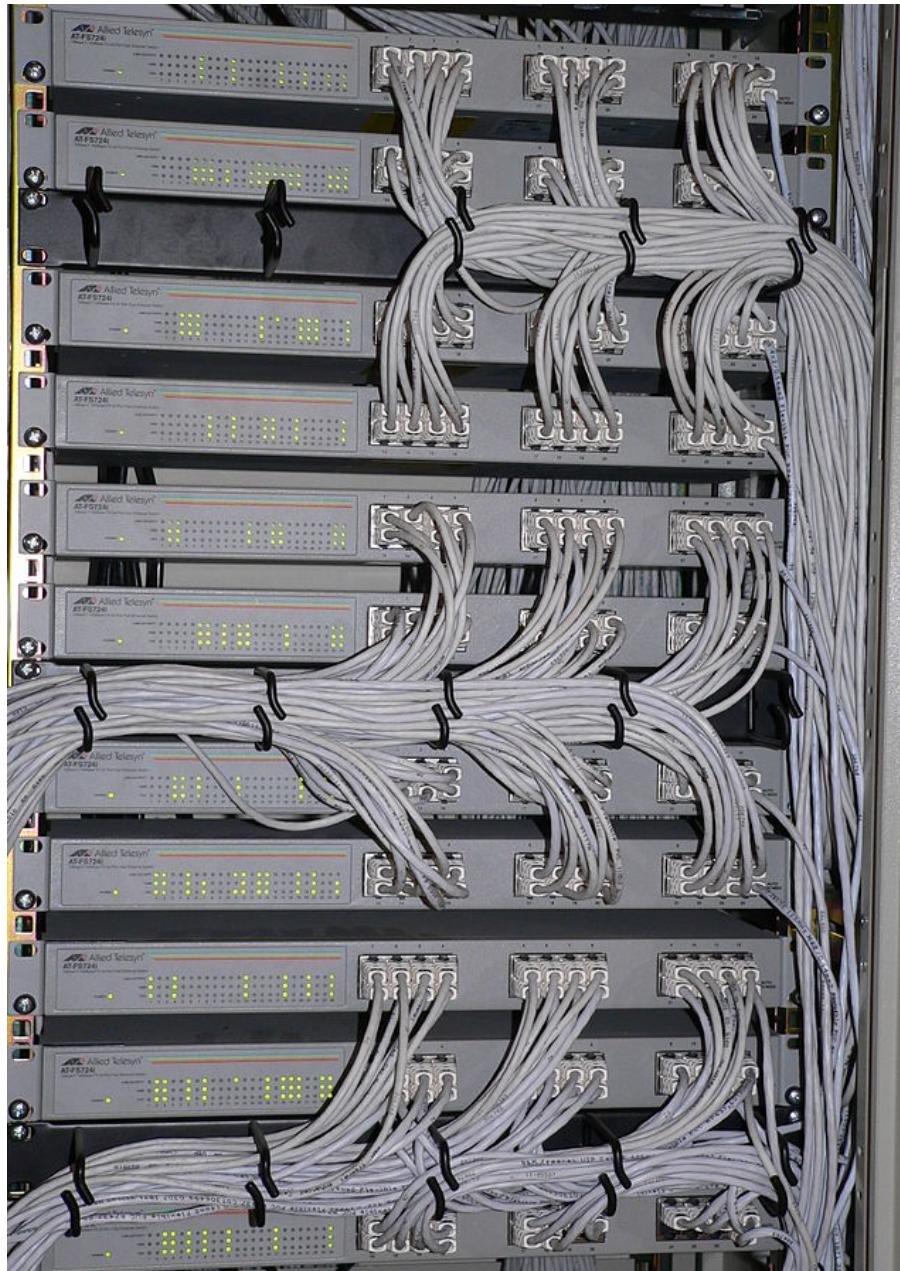
Incorrecto. Deberías volver a leerlo.

Incorrecto. Creo que necesitas un repaso.

Solución

1. Opción correcta
2. Incorrecto
3. Incorrecto
4. Incorrecto

8.2.- Dispositivos de Red.



[Parkis \(CC BY-SA\)](#)

Para crear una LAN, necesitamos seleccionar los dispositivos adecuados para conectar el dispositivo final a la red (normalmente PCs). Los dos dispositivos más comúnmente utilizados son los hubs y los switches.

e deben considerar varios factores al seleccionar un dispositivo para una LAN particular. Estos factores incluyen, entre otros:

- Costo.
- Velocidad y tipos de puertos/interfaces.
- Posibilidad de expansión.
- Facilidad de administración.
- Características y servicios adicionales.

COSTE.

El coste de un switch se determina según sus capacidades y características. La capacidad del switch incluye el número y los tipos de puertos disponibles además de la velocidad. Otros factores que afectan el costo son las capacidades de administración de red, las tecnologías de seguridad incorporadas y las tecnologías opcionales de conmutación avanzadas.

Al utilizar un simple cálculo de "coste por puerto", en principio puede parecer que la mejor opción es implementar un switch grande en una ubicación central. Sin embargo, este aparente ahorro en los costos puede contrarrestarse por el gasto generado por las longitudes de cable más extensas que se necesitan para conectar cada dispositivo de la LAN a un switch. Esta opción debe compararse con el costo generado al implementar una cantidad de switches más pequeños conectados a un switch central con una cantidad menor de cables largos.

VELOCIDAD Y TIPOS DE PUERTOS E INTERFACES.

La necesidad de velocidad está siempre presente en un entorno LAN. Se encuentran disponibles PCs más nuevos con tarjetas de red incorporadas de 10/100/1000 Mbps. La selección de dispositivos de capa 2 (por ejemplo switches) que puedan ajustarse a mayores velocidades permite a la red evolucionar sin reemplazar los dispositivos centrales.

Al seleccionar un switch, es fundamental la elección del número y tipo de puerto. Hágase las siguientes preguntas. ¿Usted compraría un switch con...?

- ¿sólo los puertos suficientes para las necesidades actuales?
- ¿una combinación de velocidades UTP?
- ¿dos tipos de puerto, de UTP y de fibra?

Considere cuidadosamente cuántos puertos UTP se necesitarán y cuántos puertos de fibra se necesitarán. Del mismo modo, considere cuántos puertos necesitarán una capacidad de 1 Gbps. y cuántos requerirán sólo anchos de banda de 10/100 Mbps. Tenga en cuenta además cuándo necesitará más puertos.

8.3.- Tipos de medios I.

Se deben considerar los diferentes tipos de medios al elegir los cables necesarios para realizar una conexión WAN o LAN exitosa. Tenemos tres alternativas:

- UTP (Categorías 5, 5e, 6 y 7).
- Fibra óptica.
- Inalámbrico.

Cada tipo de medios tiene ventajas y desventajas. Algunos de los factores que se deben considerar son los siguientes:

[Timewalk](#) (Dominio público)

Longitud del cable: ¿El cable debe atravesar una habitación o extenderse desde un edificio hasta otro?

Costo: ¿El presupuesto permite que se utilice un tipo de medios más costoso?

Ancho de banda: ¿La tecnología utilizada con los medios ofrece un ancho de banda apropiado?

Facilidad de instalación: ¿Tiene el equipo de implementación la capacidad de instalar el cable o es necesario?

Proveedor: ¿Contratar a un proveedor de servicios WAN?

Susceptibilidad a EMI/RFI: ¿Interferirá con la señal el entorno en el que estamos instalando el cable?

LONGITUD DEL CABLE.

La distancia del cableado es un factor esencial en el rendimiento de la señal de datos. La atenuación de la señal y la exposición a una posible interferencia aumenta con la longitud del cable. Cuanto más extensos sean los medios, más la atenuación afectará la señal. En algún punto, la señal no será detectable.

La longitud total del cable que se requiere para conectar un dispositivo incluye todos los cables desde los dispositivos finales del área de trabajo hasta el dispositivo de red en el rack. Esto incluye el cable desde los dispositivos finales hasta la toma de red, el cable a través del edificio desde la toma de red hasta el panel de parcheo, y el cable desde el panel de parcheo hasta el switch. Si el switch se ubica en diferentes pisos de un edificio o en diferente edificio, el cable entre estos puntos debe incluirse en la longitud total.

Para las instalaciones de cable par trenzado UTP, el estándar ANSI/TIA/EIA 568A ó B especifica que la longitud combinada total del cable que abarca las áreas enumeradas anteriormente se limita a una distancia máxima de 100 metros por enlace. Este estándar establece que se pueden utilizar hasta 10 metros de latiguillos si tenemos en cuenta que la longitud máxima de cable desde el punto de terminación en el subsistema administrador hasta la terminación en la toma del área de trabajo (roseta) no puede superar los 90 metros.

Los cables de fibra óptica pueden proporcionar una distancia de cableado mayor de hasta 500 metros o algunos kilómetros, según el tipo de tecnología. Sin embargo, el cable de fibra óptica también puede sufrir una atenuación cuando se alcanzan estos límites.

COSTO.

El costo asociado con el cableado de una LAN puede variar según el tipo de medio y es posible que el personal no pueda darse cuenta del impacto sobre el presupuesto. En un entorno ideal, el presupuesto permitiría instalar un cableado de fibra óptica para cada dispositivo de la LAN. Si bien la fibra proporciona un ancho de banda superior que el UTP, los costos de la instalación y el material son considerablemente mayores. En la práctica, generalmente no se requiere este nivel de rendimiento y no constituye una expectativa razonable en la mayoría de los entornos. Los diseñadores de redes deben lograr que coincidan las necesidades de rendimiento por parte de los usuarios con el costo de equipo y cableado para obtener la mejor relación costo/rendimiento.

ANCHO DE BANDA.

Los dispositivos de una red presentan requisitos de ancho de banda diferentes. Al seleccionar los medios para las conexiones individuales, considere cuidadosamente los requisitos de ancho de banda.

Por ejemplo, un servidor generalmente necesita mayor ancho de banda que un PC dedicado a un único usuario. Para la conexión del servidor, considere aquellos medios que proporcionarán un ancho de banda superior y que podrán desarrollarse para cumplir con mayores requisitos de ancho de banda y utilizar las tecnologías más nuevas. Un cable de fibra puede ser una elección lógica para la conexión de un servidor.

Actualmente, la tecnología utilizada en los medios de fibra óptica ofrece el mayor ancho de banda disponible entre las opciones para los medios LAN. Teniendo en cuenta el ancho de banda aparentemente ilimitado disponible en los cables de fibra, se esperan velocidades mayores para las LAN.

8.4.- Tipos de medios II.

FACILIDAD DE INSTALACIÓN.

La facilidad al instalar un cableado varía según los tipos de cables y la estructura del edificio. El acceso al piso y a sus espacios, además de las propiedades y el tamaño físico del cable, influyen en la facilidad de instalación de un cable en distintos edificios. Los cables de los edificios generalmente se instalan en canales para conductores eléctricos.

El cable UTP es relativamente liviano, flexible y tiene un diámetro pequeño, lo que permite introducirlo en espacios pequeños. Los conectores, enchufes RJ-45, son relativamente fáciles de instalar y representan un estándar para todos los dispositivos Ethernet.

Muchos cables de fibra óptica contienen una fibra de vidrio delgada. Esta característica genera problemas para el radio de curvatura del cable. La fibra puede romperse al enroscarla o doblarla fuertemente. La terminación de los conectores del cable de fibra (ST, SC,..) son mucho más difíciles de instalar y requieren de un equipo especial.

INTERFERENCIA ELECTROMAGNÉTICA/INTERFERENCIA DE RADIOFRECUENCIA

La Interferencia electromagnética (**EMI**) y la Interferencia de radiofrecuencia (**RFI**) deben tenerse en cuenta al elegir un tipo de medios para una LAN. La EMI/RFI en un entorno industrial puede producir un impacto significativo sobre las comunicaciones de datos si se utiliza un cable incorrecto.

La interferencia puede provenir de máquinas eléctricas, rayos y otros dispositivos de comunicación, incluyendo PCs y equipos de radio.

A modo de ejemplo, piense en una instalación donde los dispositivos de dos edificios distintos se encuentran interconectados. Los medios utilizados para interconectar estos edificios estarán expuestos a la posible descarga de los rayos. Además, es posible que exista una gran distancia entre estos dos edificios. La fibra óptica es la mejor elección para esta instalación.

¿FIBRA O COBRE (PAR TRENZADO)?

Se recomienda utilizar fibra en las siguientes circunstancias:

- Se conectan edificios diferentes (posible diferencia de potencial entre tierras)
- Se prevé utilizar velocidades altas o muy altas (valorar en ese caso el uso de fibras monomodo)
- Se quiere cubrir distancias de más de 100 m
- Se requiere máxima seguridad frente a intrusos (la fibra no puede 'pincharse')
- Se atraviesan atmósferas corrosivas
- Se corre el riesgo de tener fuerte interferencia electromagnética

Si no se da ninguno de estos factores es preferible utilizar cobre, ya que los equipos de emisión recepción son más baratos

Para saber más

Video tutorial Conceptos sobre sistemas de cableado estructurado, diseño y certificación

[1^a Parte](#)

[2^a Parte](#)

Información sobre tipos de cables, directrices para el tendido de cableado, instalación de cableado estructurado, verificación y comprobación, conexión de cableado RJ45...

[Cableado estructurado](#)

Si quieres conocer una aplicación muy útil para documentar mapas físicos y lógicos de redes donde se documente el de forma ilustrativa todos los detalles del diseño te recomendamos que leas el siguiente tutorial de la aplicación Visio de Microsoft:

[Curso de Visio 2003/2007](#) (pdf - 11,07 MB)

Autoevaluación

¿Cuál de las opciones siguientes constituye una fuente de interferencia en un cable UTP?

- Luces fluorescentes
- Cableado de fibra óptica.
- Switches.
- Cableado coaxial.

Las luces fluorescentes son una fuente importante de interferencias electromagnéticas que afecta a los medios de transmisión basados en el cobre (par trenzado y coaxial).

Incorrecto. Hablamos de medios basados en cobre.

Incorrecto. Pregunta por un cable.

Incorrecto. Hablamos de un cable UTP.

Solución

1. Opción correcta
2. Incorrecto
3. Incorrecto
4. Incorrecto

8.5.- Cableado de Redes.

Caso práctico

Una vez realizado el diseño y planificación de nuestra red llega el momento de llevar a cabo el diseño propuesto en el proyecto siguiendo el calendario de ejecución. En este momento se procede a la instalación y configuración de la red: Instalación de rosetas y jacks, tendido de cables, conexión de los cables en los paneles de parcheo y en las rosetas, probado de los cables, etiquetado y documentación del cable y conectores, instalación de los adaptadores de red, instalación de los dispositivos de red, etc.

Aquí no acaba el proceso, siempre queda una ligera duda sobre el buen funcionamiento de la red. Resulta lógico pensar que nuestra academia solicitaría plenas garantías de que la red va a funcionar tal como se había diseñado. Este requisito se puede cumplimentar a través de un proceso de certificación de la red.

Para saber más

Si quieras saber sobre construcción de latiguillos, montaje de roseta e instalación de redes en general te recomendamos que sigas los pasos descritos en los siguientes documentos y que vamos a tratar detalladamente en los siguientes subapartados:

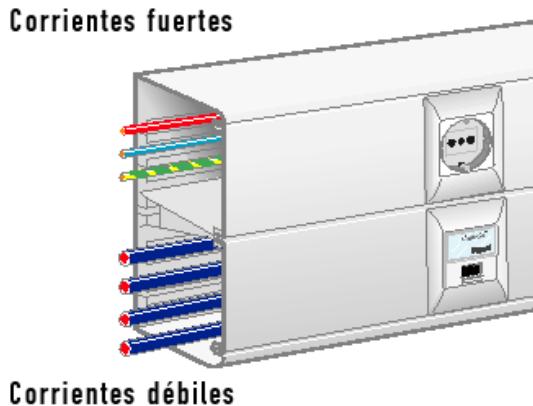
[Construcción de un latiguillo RJ-45](#) (pdf - 1,51 MB)

[Montaje de una roseta RJ-45](#) (pdf - 1,20 MB)

[Instalación física de una red](#) (pdf - 1,67 MB)

También te invitamos a ver un [video tutorial donde se explica paso a paso la forma de realizar una instalación de red](#), el cableado horizontal, latiguillos y rosetas así como la comprobación de su correcto funcionamiento.

8.5.1.- Instalación física de la Red.



[Güimi \(CC BY-SA\)](#)

La instalación consiste en la ejecución ordenada según las directrices del proyecto de instalación de un conjunto de tareas que revierten en proporcionar el servicio que el cliente que solicitó la instalación necesitaba.

Algunas de estas tareas se pueden superponer en el tiempo: es algo que habrá que tener en cuenta al confeccionar el calendario de instalación. A continuación describimos algunas de estas tareas:

Instalación de las tomas de corriente. Esta tarea suele realizarla un electricista, pero desde el punto de vista del proyecto hemos de asegurarnos de que hay tomas de corriente suficientes para alimentar todos los equipos de comunicaciones.

Instalación de conectores y tomas de red (jacks). Es la instalación de los puntos de red los puntos de red finales desde que se conectarán los dispositivos de red sirviéndose de latiguillos. La mayor parte de estas conexiones residirán en canaletas o en racks.

Canalizaciones. Se trata de decidir la forma en la que el cable se hace llegar a su destino. Se tienen que considerar diferentes canalizaciones. Algunas alternativas pueden ser:

Montaje sobre falso techo

Montaje bajo falso techo

Bandejas para cables

Canaletas de pared para el tendido de cables

Canaletas en el techo para el tendido de cables

Canaletas para rodapiés

Canaletas para repisas de ventanas

Canaletas para dinteles de ventanas

Sistemas de montaje bajo el suelo.

Sistema de montaje rápido (instalación a base de materiales prefabricados)

Armarios de comunicaciones. Paneles de parcheo. Se trata de conectar los cables en los paneles de parcheo y en las rosetas. Para ello se utiliza herramientas de crimpado apropiadas (crimpadora e impactadora).

Probado de los cables instalados. Cada cable construido y conectado debe ser inmediatamente probado para asegurarse de que cumplirá correctamente su función.

Etiquetado y documentación del cable y conectores. Todo cable debe ser etiquetado en ambos extremos así como los conectores de los paneles de parcheo y rosetas de modo que queden identificados únicamente.

Instalación de los adaptadores de red. Gran parte de los equipos informáticos vienen ya con la tarjeta de red instalada, pero esto no es así necesariamente.

Instalación de los dispositivos de red. Se trata de instalar los *hubs*, *switchs*, *routers*, etc. Algunos de estos dispositivos deben ser configurados antes de prestar sus servicios.

Tendido del cable de par trenzado.

El cable de par trenzado es muy manejable y esto hace que a veces cometamos errores o nos permitamos licencias que van a repercutir en el funcionamiento general de la red. Es conveniente seguir unas pautas generales que se pueden resumir en este gráfico.

Sobre todo hay que tener en cuenta las curvaturas que se le den (esquinas del local), cuanto y como cortemos el cable, no hacer uniones si no es estrictamente necesario, si se deben hacer, emplear los elementos de interconexión que nos proporcionen garantías en el funcionamiento de la red (nunca cinta adhesiva o similar).



[Güimi \(CC BY-SA\)](#)

8.5.2.- Elementos de la Instalación. Armarios, canaletas, suelos y techos.

La instalación de la red no solo se compone de cables y conectores. Estos deben ser fijados a las instalaciones arquitectónicas de los edificios y además hay que hacerlos convivir con instalaciones de otra naturaleza que probablemente ya hayan sido tendidas con anterioridad: agua, fuerza eléctrica, aire acondicionado, etc.

ARMARIOS Y CANALETAS

En instalaciones de tipo medio o grande, los dispositivos de red se instalan en armarios especiales que tienen unas dimensiones estandarizadas y en los que es fácil su manipulación y la fijación de los cables que a ellos se conectan. Dentro de estos armarios o **racks** se instalan paneles de parcheo para la conexión de jacks u de otro tipo de conectores. La anchura de los racks está normalizada a 19 pulgadas.

La altura de los armarios suele medirse en «U». Los fabricantes de dispositivos suelen ajustar sus equipos para que se puedan ensamblar en estos armarios ocupando 1, 2 o más «U».

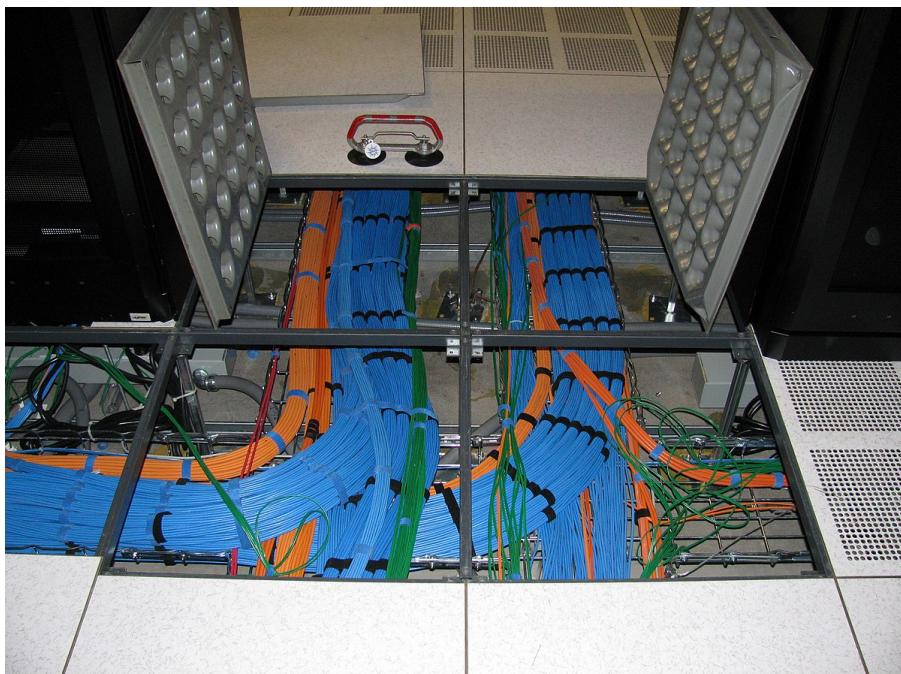
Las **canaletas** son los conductos a través de los cuales se tienden los cables para que queden recogidos y protegidos convenientemente. Hay canaletas decorativas, de aspecto más acabado cuya misión es ocultar los cables, y canaletas acanaladas que suelen instalarse en los falsos techos o falsos suelos y que son suficientemente grandes como para llevar muchos cables. Las canalizaciones de datos y de fuerza (eléctrica) suelen estar separadas para evitar interferencias.

SUELOS Y TECHOS TÉCNICOS

Las canalizaciones tendidas por suelos y techos técnicos mejoran la limpieza de la instalación haciéndola además mucho más estética.

Existen rosetas especiales para extraer de los falsos suelos tanto datos como fuerza pero en el diseño hay que poner cuidado en que no estorben al paso y en que queden protegidas para evitar su deterioro.

Los cables llegan a los armarios a través de los falsos suelos justo por debajo de ellos, lo que ayuda a la limpieza de la instalación. Los distintos cables avanzan ordenadamente normalmente embroidados, por los vértices del armario hasta alcanzar la altura a la que deben ser conectados en algún dispositivo o en algún panel de parcheo.



[Robert.Harker \(CC BY-SA\)](#)

Las canalizaciones son utilizadas para distribuir y soportar el cable y conectar equipamiento entre la salida del área de trabajo y el cuarto de telecomunicaciones. Los cables deben ir fijados en capas mediante abrazaderas colocadas a intervalos de 4 metros. Para evitar interferencias electromagnéticas la canalización de las corrientes débiles (cables de datos) debe mantenerse separada de corrientes fuertes (cables eléctricos y dispositivos electromagnéticos). Además en caso de cruzarse deben hacerlo perpendicularmente.

[Güimi \(CC BY-SA-3.0\)](#)

Para saber más

En el siguiente enlace encontrarás un interesante cuadro de distancias para las canalizaciones para distribuir y soportar el cableado de telecomunicaciones.

[Canalizaciones](#)

Autoevaluación

La altura de los racks está normalizada a 19 pulgadas.

La anchura de los armarios suele medirse en «U». Los fabricantes de dispositivos suelen ajustar sus equipos para que se puedan ensamblar en estos armarios ocupando 1, 2 o más «U»

- Verdadero Falso

Falso

La anchura de los racks está normalizada a 19 pulgadas.

La altura de los armarios suele medirse en «U». Los fabricantes de dispositivos suelen ajustar sus equipos para que se puedan ensamblar en estos armarios ocupando 1, 2 o más «U»

8.5.3.- La instalación eléctrica y de aire acondicionado.



[Estabiliza \(CC BY-SA\)](#)

Es muy importante que la instalación eléctrica esté muy bien hecha. De no ser así, se corren riesgos importantes, incluso de electrocución. Los problemas eléctricos suelen generar problemas intermitentes muy difíciles de diagnosticar y provocan deterioros importantes en los dispositivos de red.

Todos los dispositivos de red deben estar conectados a enchufes con tierra. Las carcasa de estos dispositivos, los armarios, las canaletas mecánicas, etc., también deben ser conectados a tierra.

Toda la instalación debe estar a su vez conectada a la tierra del edificio en el que habrá que cuidar que el número de picas que posee es suficiente para lograr una tierra aceptable.

Otro problema importante que hay que resolver viene originado por los cortes de corriente con las subidas y bajadas de tensión. Para ello podemos utilizar sistemas de alimentación ininterrumpida (SAI o UPS).

Normalmente, los sistemas de alimentación ininterrumpida corrigen todas las deficiencias de la corriente eléctrica, es decir, actúan de estabilizadores, garantizan el flujo eléctrico frente a cortes de corriente, proporcionan el flujo eléctrico adecuado, etc.

El SAI contiene en su interior unos acumuladores que se cargan en el régimen normal de funcionamiento. En caso de corte de corriente, los acumuladores producen la energía eléctrica que permite guardar los datos que tuvieran abiertos las aplicaciones de los usuarios y cerrar ordenadamente los sistemas operativos. Si además queremos no tener que parar, hay que instalar grupos electrógenos u otros generadores de corriente conectados a nuestra red eléctrica.

Otra necesidad muy importante en una instalación informática es el control de la temperatura y la humedad del ambiente en que se sitúan los ordenadores y otros dispositivos de red. La regulación de estos parámetros se realiza mediante la instalación de aire acondicionado. Esto reviste una especial importancia en los centros de procesos de datos (CPD).

8.5.4.- Elementos de conectividad I.

Una vez que se tiene tendido el cable en el edificio hay que proceder a realizar las conexiones utilizando conectores, rosetas, latiguillos, etc.

PANELES DE PARCHEO Y LATIGUILLOS

Un panel de parcheo es un dispositivo de interconexión a través del cual los cables instalados se pueden conectar a otros dispositivos de red o a otros paneles de parcheo.

Sobre un armario se instalan paneles de parcheo que se conectan al cableado de la instalación por todo el edificio y otros paneles de parcheo que se conectan a los conectores de los dispositivos de red, por ejemplo a los *hubs* o *switchs*.

Después, una multitud de latiguillos conectarán unos paneles de parcheo con los otros. De este modo, el cambio de configuración de cableado se realizará cambiando la conectividad del latigillo sin tener que cambiar nada del cableado largo ni las conexiones a los dispositivos de red.

El cable largo (cableado horizontal) instalado conectará las rosetas con los paneles de parcheo. Las rosetas pueden adoptar multitud de formas dependiendo del lugar en que se fijen (canaleta, pared, etc), del tipo de cable a conectar y del conector que el usuario utilizará. La roseta presenta un conector por un lado y una estructura de fijación de los cables de pares por su reverso, a la que serán crimpados.



Dsimic (CC BY-SA)

CONFECCIÓN DE LATIGUILLOS RJ45

Las estaciones de la red se conectan a los dispositivos de red a través de cables llamados latiguillos. También se utiliza para conectar los paneles de parcheo a los dispositivos de red.

Existen muchos modelos de cables de red, comentados en epígrafes anteriores, aunque recordamos algunos de ellos:

- Cable de fibra óptica.
- Cable coaxial.

Cable de par trenzado.

Nosotros nos vamos a centrar en la construcción de un latiguillo a partir de un cable de par trenzado. Dentro de los cables de par trenzado tenemos distintas categorías y modelos, vistos también en epígrafes anteriores. En concreto usaremos cable UTP categoría 5e de par trenzado no apantallado. Este tipo de cable es el idóneo para instalaciones de interior, debido a sus prestaciones y relación calidad/precio.

Si nos fijamos en el interior del cable, podemos comprobar como tenemos 8 hilos de distintos colores, agrupados en pares, en total 4 pares. Los colores que tenemos son 4 lisos:

Verde.
Naranja.
Azul.
Marrón.

Y 4 combinados:

Blanco-Verde.
Blanco-Naranja
Blanco-Azul.
Blanco-Marrón.

Lo que totalizan 8 colores.

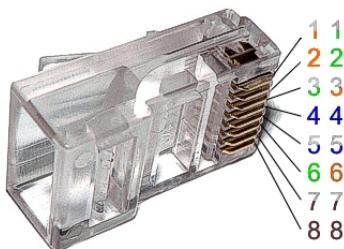
Autoevaluación

Un patch panel permite el cambio de configuración de cableado cambiando la conectividad del latiguillo dentro del patch panel, sin tener que cambiar nada del cableado largo ni las conexiones a los dispositivos de red. Similar a como se hacía en las antiguas centralitas telefónicas.

Verdadero Falso

Verdadero

8.5.4.1.- Elementos de conectividad II.



Baran Ivo (CC BY-SA)

Los colores únicamente sirven para diferenciar unos cables de otros. Son un protector de plástico y por ellos está el cable de cobre. Los 4 colores combinados se muestran mediante franjas alternas de esos dos colores.

Los extremos de los cables se introducen en conectores especiales llamados **conectores RJ45**. Para ello utilizamos una herramienta especial con forma de alicates llamadas **crimpadora**.

Este conector tiene 8 pines (contactos) de cobre, cada uno de ellos hace contacto con cada uno de los ocho hilos.

En la parte inferior posee una pestaña que evita que el conector se salga de la tarjeta de red o NIC.

Los pines se numeran del 1 al 8 empezando de izquierda a derecha (1 al 8) si miramos el conector de frente situando con los pines de cobre mirando hacia abajo y la pestaña hacia arriba. Es importante recordar esta orientación al identificar un cable.

De los ocho cables, en algunas redes *Ethernet* sólo se usan cuatro para la transmisión de señales, dos para recepción (3 y 6) y dos para transmisión (1 y 2).

Los pares azules y marrones se utilizan principalmente para alimentar electricidad a ciertos dispositivos, lo que se conoce como **PoE (Power over Ethernet)**, se utilizan los pines 4,5,7 y 8 del RJ45. Los switches que soportan PoE pueden utilizar los 4 pares para transmitir tanto datos como electricidad llegando a suministrar hasta 70W a los dispositivos que lo necesiten y soporten, por ejemplo teléfonos IP, cámaras IP o Puntos de Acceso WiFi, etc. Esto lleva una gran ventaja en ahorro de cableado de electricidad, enchufes, etc. además de facilitar la instalación de estos equipos en cualquier sitio donde solo necesitaremos una toma de datos con PoE.

Para evitar que cada uno use los colores a "su libre albedrío", la organización ANSI estableció una normativa para que sea cumplida por la mayoría de los instaladores profesionales de redes. Existen varias normativas, pero la más usada es la especificada por la ANSI/EIA/TIA-568 que es americana. Esta organización nos indica dos normativas para montaje de cable de par trenzado sobre conector RJ45. El instalador será el que decida sobre cuál de los dos usar, sobre todo si ya existe cableado o instalación anterior para reutilizar, pues deberá basarse en la que esté montada.

Las dos normativas de especificación de montaje de cable de par trenzado sobre conectores RJ45 son:

568A
568B

Según el tipo de cable que vayamos a construir (lo que se vaya a conectar), podemos tener un *cable de conexión directa* o un *cable de conexión cruzada*.

Un cable de conexión directa tiene conectores en ambos extremos usando la misma normativa en ambos extremos, ya sea la normativa T568A o la T568B.

Utilice cables directos (latiguillos) para las siguientes conexiones:

Switch a puerto *Ethernet* del router
PC a switch
PC a hub
PC a tomas de usuario (rosetas)
Dispositivo de red a panel de parcheo

Sin embargo si el cable es *cruzado*, usaremos la normativa 568A en un extremo y la 568B en el otro.

En resumen, los cables cruzados conectan directamente los siguientes dispositivos en una LAN:

Switch a switch

Switch a hub

Hub a hub

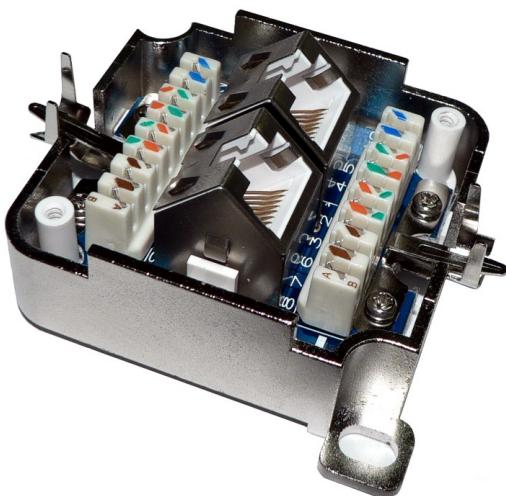
Router a conexión del puerto Ethernet del router

PC a PC

PC a puerto Ethernet del router

8.5.4.2.- Elementos de conectividad III.

CONEXIONES A ROSETAS RJ45



[Baran Ivo \(CC BY-SA\)](#)

Las rosetas (también denominadas tomas de usuario) están formadas por conectores RJ-45 hembra (*jacks* RJ-45). Estos conectores poseen por detrás 8 pines con la misma función que los conectores RJ-45 descritos en el apartado anterior. Su conexión se realiza de forma similar al conector RJ-45, sin embargo se tiene que utilizar otra herramienta denominada **impactadora o insertadora**.

ETIQUETADO DE LOS CABLES

La norma EIA/TIA-606 especifica que cada terminación de hardware debe tener alguna etiqueta que lo identifique de manera exclusiva. Un cable tiene dos terminadores, por tanto cada uno de estos extremos recibirá un nombre.

No es recomendable la utilización de un sistema de etiquetado con relación a un momento concreto, es mejor utilizar nomenclaturas neutras. Por ejemplo, si etiquetamos un PC como «PC de Dirección», y luego el lugar del edificio en donde se ubica la Dirección cambia, tendríamos que cambiar también el etiquetado, sin embargo, se trata de que el etiquetado sea fijo.

Se recomienda la utilización de etiquetas que incluyan un identificador de sala y un identificador de conector, así sabremos todo sobre el cable: dónde empieza y dónde acaba. Por ejemplo, podríamos etiquetar un cable con el siguiente identificador: **03-RS02-05RS-24**.

Este cable indicaría que está tendido desde la roseta (RS) número 02 de la sala 03 hasta la roseta 24 de la sala 05. Las rosetas en las salas 03 y 05 irían etiquetadas con 03RS02 y 05RS24 respectivamente.

Autoevaluación

¿Cuando se desarrolla una red compuesta por solo dos PC's, ¿qué tipo de cables debe usarse para conectarlos directamente?

- Cable de fibra óptica.
- Cable UTP estándar.
- Cable directo UTP.
- Cable cruzado UTP

Incorrecto. Sería excesivo.

No es correcto, el estándar no serviría.

Incorrecto. Así no vas a conseguir comunicación.

El cable cruzado se emplea para conectar dos equipos directamente.

Solución

1. Incorrecto
2. Incorrecto
3. Incorrecto
4. Opción correcta

¿Cuando se tiende un cable desde el armario para el cableado a los jacks de pared (roseta) ¿dónde se encuentra rotulado dicho cable?

- En cada atadura.
- En cada extremo.
- En el extremo del jack.
- En el extremo del panel.

No es correcto, ¿qué entiendes por atadura?

Los cables horizontales (van desde los paneles de parcheo hasta las rosetas) deben ir etiquetados en los dos extremos.

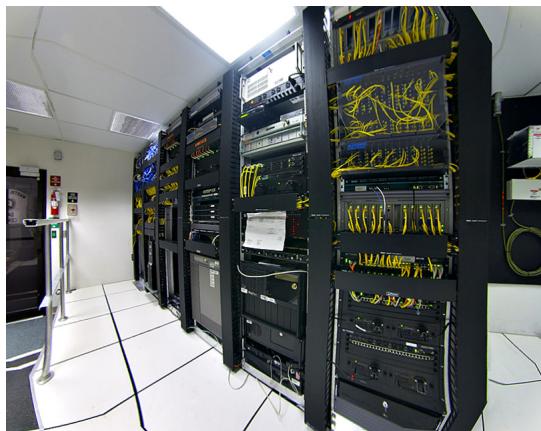
Incorrecto. ¿Cuál es el extremo de Jack?

Incorrecto. No sería suficiente.

Solución

1. Incorrecto
2. Opción correcta
3. Incorrecto
4. Incorrecto

8.5.5.- Instalación del Centro de Proceso de Datos.



[MickStephenson \(CC BY-SA\)](#)

Se denomina centro de procesamiento de datos (CPD) a aquella ubicación donde se concentran todos los recursos necesarios para el procesamiento de la información de una organización.

Un CPD es un edificio o sala de gran tamaño usada para mantener en él una gran cantidad de equipamiento electrónico. Suelen ser creados y mantenidos por grandes organizaciones con objeto de tener acceso a la información necesaria para sus operaciones. Por ejemplo, un banco puede tener un data center con el propósito de almacenar todos los datos de sus clientes y las operaciones que estos realizan sobre sus cuentas. Prácticamente todas las compañías que son medianas o grandes tienen algún tipo de CPD, mientras que las más grandes llegan a tener varios.

Entre los factores más importantes que motivan la creación de un CPD se puede destacar el garantizar la continuidad del servicio a clientes, empleados, ciudadanos, proveedores y empresas colaboradoras, pues en estos ámbitos es muy importante la protección física de los equipos informáticos o de comunicaciones implicados, así como servidores de bases de datos que puedan contener información crítica.

El diseño de un centro de procesamiento de datos comienza por la elección de su ubicación geográfica, y requiere un balance entre diversos factores:

Coste económico: coste del terreno, impuestos municipales, seguros, etc.

Infraestructuras disponibles en las cercanías: energía eléctrica, carreteras, acometidas de electricidad, centralitas de telecomunicaciones, bomberos, etc.

Riesgo: posibilidad de inundaciones, incendios, robos, terremotos, etc.

Una vez seleccionada la ubicación geográfica es necesario encontrar unas dependencias adecuadas para su finalidad, ya se trate de un local de nueva construcción u otro ya existente a comprar o alquilar. Algunos requisitos de las dependencias son:

Doble acometida eléctrica.

Muelle de carga y descarga.

Montacargas y puertas anchas.

Altura suficiente de las plantas.

Medidas de seguridad en caso de incendio o inundación: drenajes, extintores, vías de evacuación, puertas ignífugas, etc.

Aire acondicionado, teniendo en cuenta que se usará para la refrigeración de equipamiento informático.

Almacenes.

Etc.

Aún cuando se disponga del local adecuado, siempre es necesario algún despliegue de infraestructuras en su interior:

- Falsos suelos y falsos techos.
- Cableado de red y teléfono.
- Doble cableado eléctrico.
- Generadores y cuadros de distribución eléctrica.
- Acondicionamiento de salas.
- Instalación de alarmas, control de temperatura y humedad con avisos SNMP o SMTP.
- Etc.

Una parte especialmente importante de estas infraestructuras son aquellas destinadas a la seguridad física de la instalación, lo que incluye:

- Cerraduras electromagnéticas.
- Torniquetes.
- Cámaras de seguridad.
- Detectores de movimiento.
- Tarjetas de identificación.
- Etc.

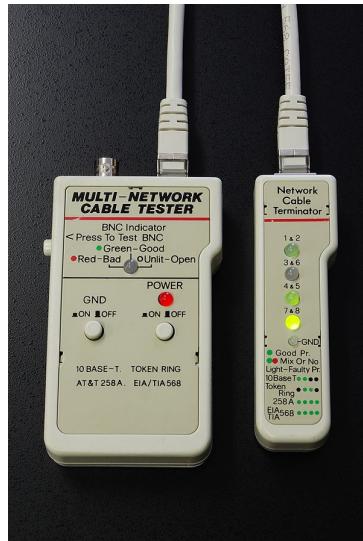
Una vez acondicionado el habitáculo se procede a la instalación de las computadoras, las redes de área local, etc. Esta tarea requiere un diseño lógico de redes y entornos, sobre todo en aras a la seguridad. Algunas actuaciones son:

- Creación de zonas desmilitarizadas(DMZ).
- Segmentación de redes locales y creación de redes virtuales (VLAN).
- Despliegue y configuración de la electrónica de red: pasarelas, encaminadores, conmutadores, etc.
- Creación de los entornos de explotación, pre-explotación, desarrollo de aplicaciones y gestión en red.
- Creación de la red de almacenamiento.
- Instalación y configuración de los servidores y periféricos.
- Etc.

Generalmente, todos los grandes servidores se suelen concentrar en una sala denominada "sala fría", "nevera", "pecera" (o site). Esta sala requiere un sistema específico de refrigeración para mantener una temperatura baja (entre 21 y 23 grados centígrados*), necesaria para evitar averías en las computadoras a causa del sobrecalentamiento.

La "pecera" suele contar con medidas estrictas de seguridad en el acceso físico, así como medidas de extinción de incendios adecuadas al material eléctrico, tales como extinción por agua nebulizada o bien por gas INERGEN, dióxido de carbono o nitrógeno.

8.5.6.- Certificación de la Instalación.



[Smial \(CC BY-SA\)](#)

El correcto funcionamiento del sistema de cableado es tan importante que en muchas instalaciones se exige la certificación de cada uno de los cables, es decir, se compara la calidad de cada cable con unos patrones de referencia propuestos por un estándar. En el caso de los cables de cobre, la norma comúnmente utilizada es la ANSI/TIA/EIA-TSB-67 del año 1995, la norma EIA/TIA 568 y su equivalente norma ISO IS11801.

La certificación de una instalación significa que todos los cables que la componen cumplen con esos patrones de referencia y, por tanto, se tiene la garantía de que cumplirán con las exigencias para las que fueron diseñados. Las consideraciones del EIA/TIA 568 especifican los siguientes elementos:

Requerimientos mínimos para el cableado de telecomunicaciones.

Topología de la red y distancias máximas recomendadas.

Parámetros determinantes del rendimiento.

La certificación de cables consiste en utilizar un dispositivo certificador de cables para comprobar el buen estado de algunos cables. Para ello, hay que seguir las indicaciones que el fabricante del dispositivo nos proporcionará en el manual de operación o de usuario. Se sugiere la certificación de la instalación de la red, pero si no es posible se tendrán que confeccionar nuevos cables para su comprobación.

Autoevaluación

¿Para que un gerente de red pueda realizar la instalación de una nueva red, ¿cuál de los siguientes elementos serán necesarios para implementar una instalación de red 100BASE-TX típica?

RJ-11.

Conectores BNC.

Cables de conexión RJ-48

Conectores RJ-45

Cables UTP de categoría 5e

Swithes

[Mostrar retroalimentación](#)

Solución

1. Incorrecto
2. Incorrecto
3. Incorrecto
4. Correcto
5. Correcto
6. Correcto

Autoevaluación

¿Las herramientas para fabricar y comprobar un latiguillo de par trenzado son?

- Crimpadora, cortador y pelador.
- Crimpadora, cortadora, peladora y testers
- Crimpador, cortador, pelador, testers e insertadota.
- Crimpador, cortador, pelador e insertadota.

No es correcto. Falta algo para comprobar.

Siempre que vayamos a rea lizar un cable de red de conexión paralela o latiguillo (patch cord) necesitamos como materiales: cable UTP Cat 5e, conectores RJ-45 y crimpadora. Normalmente la crimpadora suele llevar incorporada peladora y cortadora.

Incorrecto. Creo que para el latiguillo sobra alguna.

Incorrecto. Pedimos también la comprobación.

Solución

1. Incorrecto
2. Opción correcta
3. Incorrecto
4. Incorrecto

Para saber más

Puedes completar este apartado en el siguiente enlace de Güimi, donde encontrarás además interesantes ilustraciones y ejemplos que te ayudarán a entender estos conceptos.

[Instalación de cableado estructurado.](#)

También recomendamos que visites el siguiente enlace del IES Haría de Las Palmas, en el que han hecho una estupenda recopilación de la principal normativa sobre cableado estructurado.

[Normativa y estándares aplicables a los Sistemas de Cableado Estructurado](#)

Condiciones y términos de uso de los materiales

Materiales desarrollados inicialmente por el Ministerio de Educación, Cultura y Deporte y actualizados por el profesorado de la Junta de Andalucía bajo licencia Creative Commons BY-NC-SA.

Antes de cualquier uso leer detenidamente el siguiente [Aviso legal](#)

Historial de actualizaciones

Versión: 02.00.01

Fecha de actualización: 19/10/21

Actualización de materiales y correcciones menores.

Versión: 02.00.00

Fecha de actualización: 21/06/21

Autoría: Jesús Manuel Marín Navarro

Ubicación: Todo

Mejora (tipo 1): Revisado todo

Ubicación: 5.2

Mejora (tipo 1): Para empezar hay que entrar al modo especial de administración de la base de datos VLAN y desde ahí configurar el número de versión VTP que usaremos. Desde este modo también se pueden crear VLANs como una forma alternativa a la vista en el apartado 2.2

Ubicación: Videoconferencia

Mejora (tipo 1): Como propuesta para añadir al temario, voy a incluir una iniciativa que llevo añorando desde que empecé el estudio, no solo de este módulo, sino de otros en los que estoy matriculado. Y es que se da por asumido el conocimiento previo del alumno en muchas materias. Y no es mi caso, como supongo que no será en el caso de algunos de mis compañeros y compañeras. Propongo en este tema que se realice una actividad, que puede ser una videoconferencia (no para solucionar dudas o para que Jesús nos de algunas indicaciones). Sino la Videoconferencia sería un apartado más del temario en donde nos enseñe como funciona el programa Packet Tracer solo y exclusivamente.

Al principio de empezar este tema, me atasqué mucho en el funcionamiento del programa, pero la videoconferencia que tuvimos me aclaró como funcionaba y para que servía. Porque hasta ese momento no tenía ni idea de como funcionaba el programa. Intenté hacer un ejemplo sencillo con un router y dos equipos y no logré ni que se pusieran en verde ninguna de las conexiones. No todos somos expertos en Packet Tracer y si va a ser una herramienta que debemos tener soltura al manejarla, tanto como para ser la base del examen presencial o telemático en Febrero y supongo que en Junio también, es necesario que nos enseñen a como manejarlo.

Ubicación: Todo el tema

Mejora (tipo 3): Hacer una introducción hablando sobre la industria/sector de las redes y sus diversos actores dónde se trabaja con equipos de redes de diversas formas: Organismos de Estandarización, Fabricantes, Socios integradores (Partners), Proveedores de Servicio (ISP), Grandes Empresas (Enterprise), Pequeña y Mediana Empresa (SOHO), etc. En el apartado 3 hacer referencia de nuevo a los organismos de estandarización.

Apartado 1: Hacer una mejor clasificación de las redes según distintos criterios (como en materiales de SMR)

En apartado 2: Poner más ejemplos, hacerlo más claro, plantear algún ejercicio resuelto de conversiones. Hablar sobre las unidades de medida (K, M, G, T, etc.) como he añadido al apartado 2 de la unidad 2

Añadir vídeos de Sistemas numéricos

<https://www.youtube.com/watch?v=g9-MRBBcvdg&feature=youtu.be>
https://www.youtube.com/watch?v=QrULhy0P_uU&feature=youtu.be
<https://www.youtube.com/watch?v=c-hyLLdDt7I>

<https://www.youtube.com/watch?v=IqFaPj6BYi4> (más actualizado)

Apartados 3, 4 y 5: Repasarlo entero en general para hacerlo más didáctico y fácil de entender.

Coger ideas de los materiales de SMR que está mucho mejor explicado y resumido

Vídeo introductorio a arquitecturas OSI y TCP/IP <https://www.youtube.com/watch?v=jdKRx2BxSMs>

5.2.4 hablar también de CSMA/CA en WiFi y CSMA/CR en redes CAN (de máquinas y coches)

<https://www.ionos.es/digitalguide/servidores/know-how/csmaca-protocolo-de-acceso-al-medio-para-redes-inalambricas/>

Apartado 6 - Rapasarlo entero en general

6.2 : cambiar el gráfico por otro que se vea mejor la diferencia entre lo que es IP, TCP, etc.

6.2.1 : confunde trama con paquete en varias ocasiones

6.2.2 : Explicar mejor los usos de la 0.0.0.0

6.2.3 : Cambiar fragmento por segmento . IGMP es para multicast

6.3.1 : cambiar trama TCP por segmento TCP

6.3.2 : cambiar esa imagen que no viene a cuento

6.1 - Referenciar también a todo lo visto en el apartado 4 y 5, de capa física y de enlace

6.2.2 - Darle más importancia, mejor explicado y actualizado, con más ejemplos, etc. Introducir IPv6 (sí se ve algo en Unidad 2). Coger ideas de la Unidad 5 que modifiqué de SMR. Hacer nuevos apartados explicando las máscaras y ejemplos resueltos de ejercicios.

Vídeo IPs <https://www.youtube.com/watch?v=SHbBso63X38>

Video VLSM : <https://www.youtube.com/watch?v=0LyItIZejvA>

Crear subredes: https://www.youtube.com/watch?v=sLWYpqjT0_Y

otro subredes:

https://www.youtube.com/watch?v=sLWYpqjT0_Y

6.3.2 - explicar que hay puertos reservados, cómo se deciden los puertos de origen/destino, que son de 16 bits, etc. Explicar comandos de netstat para ver los puertos que usa un determinado servicio en Windows y Linux para resolver conflictos de puertos ocupados en un servidor.

Apartado 7: Que quede claro que se va a hablar de tipos de LAN, y algunas de ellas históricas...

El 7.3 hay que revisarlo y actualizarlo entero...

*** Habría que reordenar los apartados o la estructura del tema, porque se habla de Ethernet en varios sitios desordenados a partir del apartado 8.

El apartado 8. también actualizar con las nuevas tecnologías. Y asociar cada capa física con su correspondiente protocolo de enlace!

En el 9. lo comenta algo de esa asociación pero no hace una buena tabla que lo deje claro y actualizado.

Apartado 11:

El cableado se trata en varios apartados pero no se habla de las diferentes Categorías actualizadas.

Hablar del mGig para sin recablear (Cat 5e o 6) usar velocidades superiores al Gbps

No se profundiza en la fibra óptica y sus diferentes tipos y conectores.

Aquí hay más info sobre cableado estructurado <http://platea.pntic.mec.es/~lmarti2/cableado.htm>

Los apartados 12 y 13 habría que reordenarlos dentro de un gran apartado de Ethernet

El tema se hace largo y muy teórico en ocasiones. Hay que enfatizar y resaltar lo que es necesario e importante memorizar y comprender, y separarlo de lo que está como referencia y que es bueno "que les suene". Separar en secciones de "Para Saber más", "Debes Saber", etc.

Incluir una referencia final (Anexo?) a la película "Warriors of the Net" como en apartado 3.5 de SMR. Indicando los errores de concepto que tiene.

Ubicación: 6.2.3

Mejora (tipo 1): IGMP es para multicast

Ubicación: 6.2.2

Mejora (tipo 1): aclarar la 0.0.0.0 : Tiene varios usos como se puede ver en Wikipedia. Puede representar tanto todas las IPs como ninguna según el contexto. También se utilizaba cuando se están arrancando las estaciones, hasta la carga del sistema operativo, luego no se usa.

Antiguamente se usaba también cuando no se obtenía una dirección mediante DHCP, pero ahora se usa APIPA en sistemas operativos Windows entre otros.

Ubicación: 8, 10, 12 y 13

Mejora (tipo 2): Distinguir bien y hablar de los diferentes estándares de cableado y protocolos 802.3.

Está mal explicado, mal explicitado y no está bien categorizado, separado, etc.
Se habla de las mismas cosas en sitios distintos pero no se relacionan...

Ubicación: 5.2.4

Mejora (tipo 2): Explicar también CSMA/CA usado en WiFi

Ubicación: 6.4

Mejora (tipo 2): Explilar mejor esta capa tan importante y Añadir Debes Conocer con :

El protocolo más típico de esta capa es el HTTP (o HTTPS para usar comunicaciones seguras mediante SSL) que permite a los navegadores web (Firefox, Chrome, etc.) comunicarse e intercambiar páginas web (escritas en lenguaje de marcas HTML) y todo tipo de contenido con los servidores web (como por ejemplo Apache, NGINX, IIS, etc.) que escuchan por defecto en el puerto 80 (ó 443 para HTTPS).

Ubicación: 5.7

Mejora (tipo 1): Está mal lo de las aplicaciones... la capa de aplicación son los protocolos que usarán las aplicaciones...

Ubicación: 6.3.2

Mejora (tipo 1): cambiar esa imagen que no viene a cuenta

Ubicación: 6.3.1

Mejora (tipo 1): cambiar trama TCP por segmento TCP

Ubicación: 6.2.3

Mejora (tipo 1): Cambiar fragmento por segmento

Ubicación: 1.1.1

Mejora (tipo 1): Cambiar peer to peer por peer to peer

Ubicación: 6.2

Mejora (tipo 1): cambiar el gráfico por uno que se vea mejor la diferencia entre lo que es IP, TCP, etc.

Ubicación: 6.2.1

Mejora (tipo 1): confunde trama con paquete en varias ocasiones

Ubicación: Todo

Mejora (Mapa conceptual): Revisado todo

Ubicación: 1

Mejora (Orientaciones del alumnado): Actualizado el índice

Versión: 01.00.00

Fecha de actualización: 23/07/20

Versión inicial de los materiales.

