CONCEPTOS DE REDES

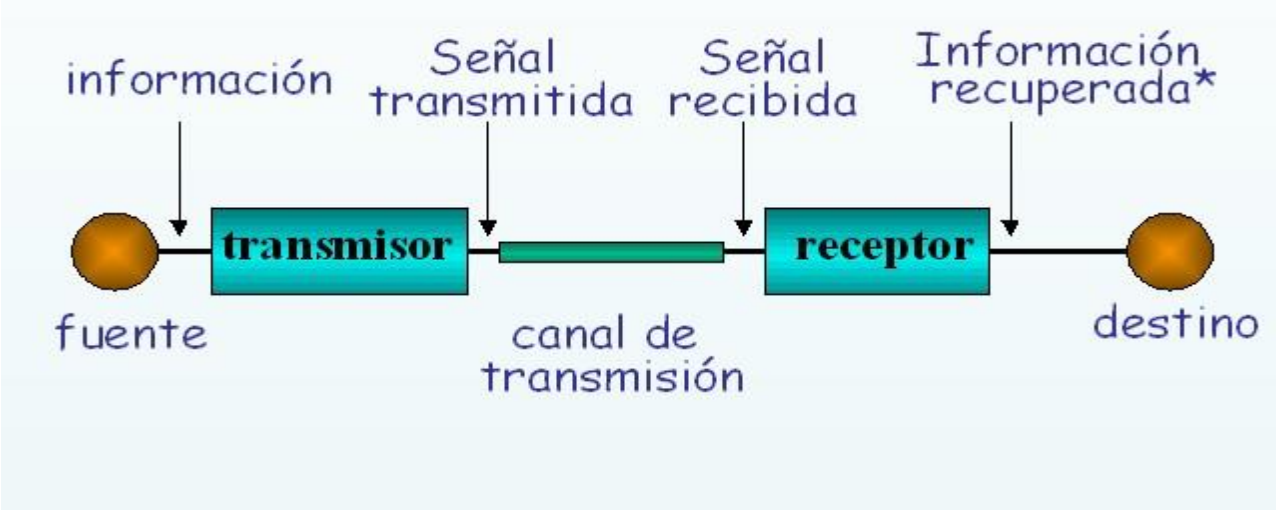
Contenido

TRANSMISIÓN DE DATOS

CARACTERISTICAS DE LA TRANSMISION DE DATOS

Se denomina transmisión de datos al proceso por el cual una información codificada mediante señales eléctricas, ópticas, electroópticas y electromagnéticas viaja a través de un medio canal de un punto a otro o de un punto a un multipunto.

Para comunicar dicha información se requieren 4 elementos:



- **Fuente y Destino:** son los sistemas finales o también llamados **Equipos Terminales de Datos** (ETD). La **fuente** es de donde proviene la información y son recibidos por el **destino**, que es el receptor final de la información.

- **Información o mensaje:** conformado por los datos trasmitidos que pueden ser analógicos o digitales. Los **datos analógicos** toman valores en un determinado intervalo continuo, como la temperatura medida por un sensor; sin embargo, los **datos digitales** toman valores discretos, como los valores 0 o 1, o los enteros de 0 a 255.

- **Transmisor y Receptor:** también llamados **Equipos Terminales de Circuito de Datos** (ETCD), el **transmisor** se encarga de adaptar la señal de los datos para enviarlos bajo presencia de interferencia y el **receptor** se encarga de recibir datos y recuperar los datos afectados por interferencias, para luego regresarlos a su estado original.

- **Medios o canales:** caminos físicos o lógicos por medio de los cuales viaja la información entre la fuente y el destino.

TIPOS DE SEÑAL

Señal analógica

Una señal se clasifica como **analógica** cuando su amplitud puede tomar un infinito número de valores en un rango continuo de tiempo.

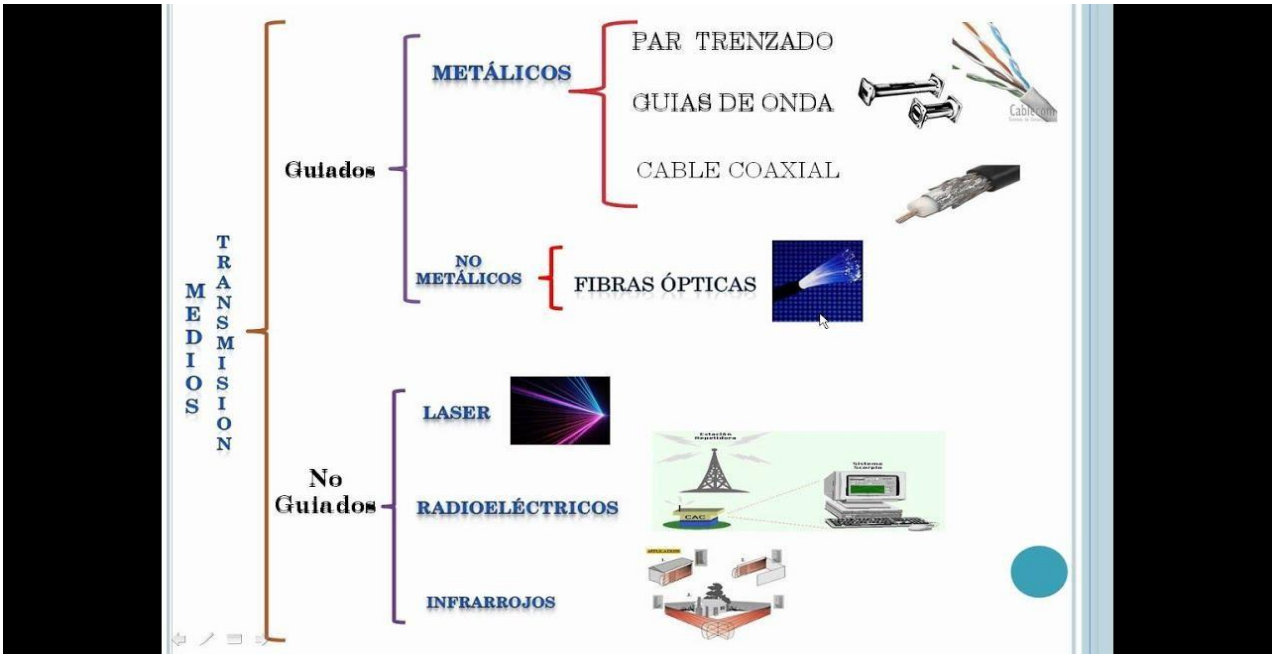
Señal digital

Una señal se clasifica como **digital** cuando la amplitud puede tomar solo un número finito de valores, para un número finito de muestras en el tiempo.

CANAL O MEDIO DE COMUNICACIÓN

Se define como el medio por el cual son transmitidos los datos contenidos en una señal desde un punto a otro. Los medios de transmisión se clasifican en **alámbricos** e **inalámbricos**. En ambos casos, la comunicación se lleva a cabo con ondas electromagnéticas. En los medios **alámbricos** las ondas se confinan en un medio sólido, como por ejemplo: par trenzado, cable coaxial, fibra óptica.

Ejemplos de medios **inalámbricos** son la atmósfera o espacio exterior, que proporcionan un medio de transmitir las señales, pero sin confirmarlas; este tipo de transmisión se denomina inalámbrica Dentro de éstas están: Telefonía celular, Satélites y Antenas.



TIPOS DE TRANSMISION

Simplex o Unidireccional

Es aquel en el que una estación siempre actúa como fuente y la otra siempre como colector, este método permite la transmisión de información en un único sentido. Un ejemplo de transmisión simplex es la señal que se envía de una estación de TV a la TV de su casa.

Half-duplex

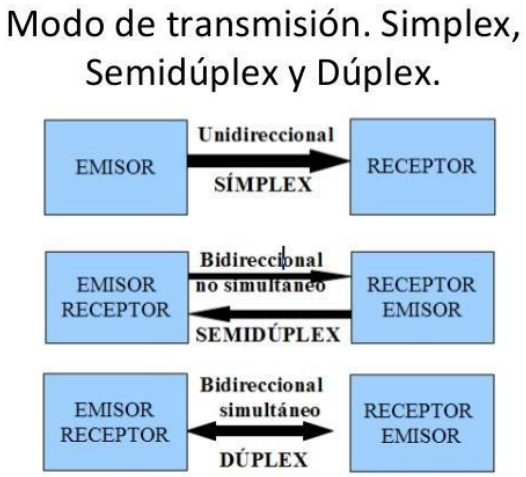
Es aquel en el que una estación A en un momento de tiempo, actúa como fuente y otra estación corresponsal B actúa como colector, y en el momento siguiente, la estación B actuará como fuente y la A como colector. Permite la transmisión en ambas direcciones, aunque en momentos diferentes.

Ejemplo, Las radios bidireccionales, como las radios móviles de comunicación de emergencias o de la policía, funcionan con transmisiones half-duplex. Cuando presiona el botón del micrófono para transmitir, no puede oír a la persona que se encuentra en el otro extremo. Si las personas en ambos extremos intentan hablar al mismo tiempo, no se establece ninguna de las transmisiones.

Full-duplex

En lo esencial es similar al método anterior, en el que dos estaciones A y B, actúan como fuente y colector, transmitiendo y recibiendo información simultáneamente. permite la transmisión en ambas direcciones y de forma simultánea.

Por ejemplo, una conversación telefónica, en donde ambas personas pueden hablar y escucharse al mismo tiempo.



FORMAS DE TRANSMISION

Sincrónica

La transmisión es sincrónica cuando una existe coordinación temporal precisa entre emisor y receptor. En este tipo de transmisión no hay bits de comienzo ni de parada, por lo que se transmiten bloques de muchos bits (aun en el caso que no haya caracteres a transmitir, la sincrónica se mantiene y es frecuente que se envíen continuamente bits llamados de “relleno”). Por ejemplo: una llamada telefónica.

Asincrónica

Se dice que una transmisión es asincrónica cuando no hay coordinación temporal estricta entre el emisor y el receptor. Es decir, el ritmo de presentación de la información no tiene por qué coincidir con el ritmo de presentación de la información por la fuente.

En este tipo de transmisión el receptor no sabe con precisión cuando recibirá el mensaje. Por ejemplo: el correo electrónico, mensajes de texto.

Elemento	Sincrónico	Asincrónico
Emisor	Envía la información sabiendo que obtendrá una respuesta inmediata	Envía la información sabiendo que no obtendrá una respuesta inmediata
Receptor	Es consciente de la llegada del mensaje, al utilizar el canal especifico	Será consciente de la llegada del mensaje, sólo cuando acceda al canal especifico
Canal	Medio Físico acordado por ambas partes por el que se trasmite el mensaje, no deberá ser perdurable en el tiempo, ya que no hay necesidad de mantenerlo indefinido.	Medio Físico acordado por ambas partes por el que se trasmite el mensaje, debe ser perdurable en el tiempo, ya que el mensaje se almacena allí durante un tiempo indefinido.
Contexto	Contenido fluido.	Contenido expectante, de acuerdo a la necesidad del receptor.
Retroalimentación	Hay respuesta inmediata.	Existe incertidumbre para conocer la respuesta, cuando es necesaria.

VELOCIDAD DE TRANSMISION

La velocidad de transmisión de datos es un promedio del número de bits, caracteres o bloques que se transfieren entre dos dispositivos, por una unidad de tiempo, usualmente segundos.

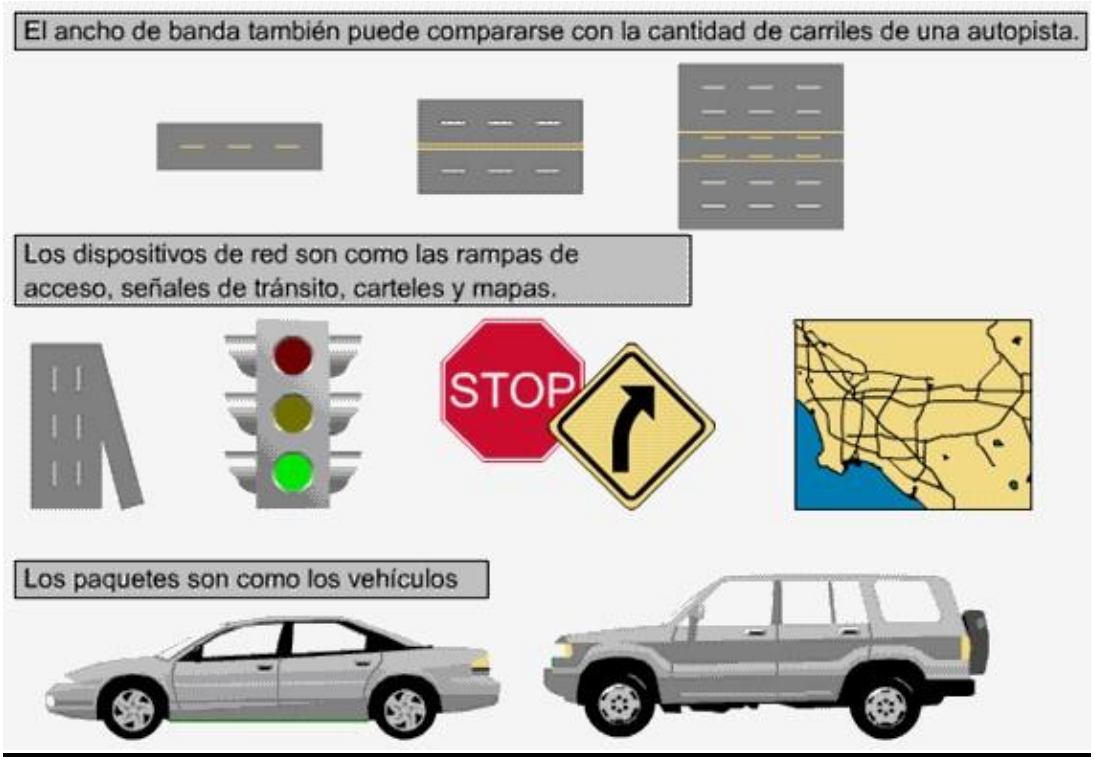
En otras palabras, es la cantidad de datos digitales que son movidos de un lugar a otro en un determinado tiempo. En general, mientras más grande sea el ancho de banda de un determinado canal o camino, más elevada será la velocidad de transmisión de datos.

ANCHO DE BANDA

El ancho de banda se mide como la cantidad de datos que se pueden transferir entre dos puntos de una red en un tiempo específico. Normalmente, el ancho de banda se mide en bits por segundo (bps) y se expresa como una tasa de bits.

El ancho de banda denota la capacidad de transmisión de una conexión y es un factor importante al determinar la calidad y la velocidad de una red.

Hay varias formas diferentes de medir el ancho de banda. Algunas se utilizan para calcular el flujo de datos en un momento dado, mientras que otras miden el flujo máximo, el flujo típico o lo que se considera un buen flujo.



Importancia del ancho de banda

La importancia del ancho de banda se basa en la necesidad del transporte de información según la capacidad que se requiera.

Es importante entender que:

- Es finito.
- No es gratuito.
- Es un factor clave a la hora de analizar el rendimiento de una red, diseñar nuevas redes y comprender la internet.
- Es fundamental para el desempeño de la red.

VELOCIDAD DE TRANSFERENCIA

La velocidad de transferencia es la cantidad de datos digitales que se mueve de un lugar a otro en un momento dado, en otras palabras, la velocidad de transferencia de datos es la velocidad a la que se transmiten los datos entre diferentes medios o dispositivos tales como módem, ethernet, USB, DVD, CD, etc.

En una conexión de red informática se mide normalmente en unidades de bits por segundo (bps), kilobits por segundo (kbps), megabits por segundo (mbps), gigabit por segundo (Gbps) o terabit por segundo (PDD).

La Velocidad de Transferencia entonces se desglosa en dos conceptos fundamentales:

- **Velocidad de Transferencia Constante (CBR)**: La cantidad de datos enviados es uniforme, por lo que no se tienen en cuenta los factores anteriormente mencionados, ni la densidad de información que es enviada en uno u otro momento

- **Velocidad de Transferencia Variable (VBR):** En este caso, la medición no es uniforme sino que se realiza una diferencia entre las zonas de menor o mayor densidad, siendo entonces una cantidad mucho más precisa

VELOCIDAD REAL DE TRASFERENCIA DE DATOS

Es el número medio de bits por unidad de tiempo que se transmiten entre los equipos de un sistema de transmisión de datos, a condición de que el receptor de estos acepte como válidos, es decir, que no se tienen en cuenta los errores de transmisión.

TASA DE ERROR

El BER (Tasa de Error de Bits) nos da una indicación de cuando un paquete, u otra unidad de datos, tiene que ser retransmitida a causa de un error. Un BER muy alto, puede indicar que una velocidad menor de los datos podría reducir el tiempo de transmisión para una determinada cantidad de datos, ya que un BER más bajo reduciría la cantidad de paquetes que deban ser retransmitidos.

Un concepto relacionado es el BERT (Bit Error Rate Test o Tester) que es un procedimiento o dispositivo que mide el BER para una transmisión.

Redes: Medios de Transmisión

Es un conjunto de equipos conectados por medio de cables, señales, ondas, o cualquier otro método de transporte de datos, que compartan información, archivos, recursos (CD – ROM, impresoras, etc.) o servicios (acceso a internet, etc.).

También es definido como un conjunto de medios técnicos que permiten la comunicación a distancia entre equipos autónomos.

Transmisión

La transmisión de datos implica al movimiento de información codificada, de un punto a uno o más puntos, mediante señales eléctricas, ópticas, electroópticas o electromagnéticas. Las tecnologías actuales de transmisión usan ondas electromagnéticas o pulsos de luz. En el caso de las terrestres los datos se conducen a través de cables. En los medios aéreos, se utiliza el aire como medio de transmisión, a través de radiofrecuencias, microondas y luz (infrarrojos, láser).

Clasificación de las redes

Existen varios tipos de redes las cuales se pueden clasificar según su alcance, su método de conexión, y su relación funcional. En este caso se les clasificara por método de conexión, las cuales se dividen en red aérea y terrestre.

Red terrestre

Una red terrestre está formada por la conexión de cables entre los distintos dispositivos que lo conforman. Entre las cuáles tenemos:

1. Cable coaxial (CATV)
2. Cable de par trenzado (DSL)
3. Fibra óptica (Broadband Trunk)

Medios de transmisión terrestre

Cable Coaxial

El cable coaxial permite conducir electricidad y está recubierto por una envoltura compuesta por varias capas, está fabricado con conductores eléctricos como el aluminio o el cobre. Este tipo de cable se utiliza para transmitir señales de electricidad de alta frecuencia. Estos cables cuentan con un

par de conductores concéntricos: el conductor vivo o central que está destinado a transportar los datos, y el conductor exterior, blindaje o malla, el cual actúa como retorno de la corriente y referencia de tierra. Entre ambos se sitúa una capa aisladora. Se utiliza para TV por cable y redes de área local. Utilizado en telefonía de sistemas, pero la fibra óptica ahora está asumiendo esta tarea.

Principales ventajas

- Capacidad para ofrecer transferencias de datos con un gran ancho de banda
- Alto blindaje: excelente robustez de EMC
- Proceso de montaje automatizado de conectores
- Cumplimiento de los exigentes requisitos mecánicos, como capacidad de flexión y amplio rango de temperatura
- Solución económica homologada para el automóvil
- Impedancia altamente controlada que permite el modo de funcionamiento full-dúplex.
- Permite transmitir alimentación y transmisión de datos a través del mismo cable.

Usos típicos

Se puede encontrar un cable coaxial:

- En las redes urbanas de televisión por cable e internet.
- Entre un emisor y su antena (equipos de radioaficionados).
- Entre líneas de distribución de señal de video.
- En las redes de transmisión de datos como Ethernet en sus antiguas versiones.
- En las redes telefónicas interurbanas y en los cables submarinos.
- Cables de transmisión submarinos.

Cable par trenzado

Un Par Trenzado consiste en 2 cables de cobre aislado, los cuales están unidos entre sí de forma similar a una estructura de ADN; esta forma trenzada se utiliza para reducir la interferencia eléctrica entre dos o más pares de cobre o bien interferencias del exterior. Debido a su fácil instalación, velocidad de transmisión de hasta varios Mbps y bajo coste, los pares trenzados se utilizan ampliamente.

Dependiendo de la forma en que se agrupen los pares, encontramos:

- **Pares trenzados no apantallados (UTP):** son los más simples. El par trenzado UTP categoría 5 está recubierto de una malla de teflón que no es conductora.

- **Pares trenzados apantallados individualmente (STP):** iguales a los anteriores, pero cada par rodeado de una malla conductora, que se conecta a las diferentes tomas de tierra de los equipos. Poseen mayor inmunidad al ruido.

- **Pares trenzados apantallados (FTP):** Cables pares que poseen una pantalla conductora global en forma trenzada. Mejora la protección frente a interferencias.

Así mismo, dependiendo del número de pares que tenga un cable, el número de vueltas por metro que posee su trenzado y los materiales utilizados, los estándares de cableado clasifican a los pares trenzados por distintas categorías.

Principales ventajas

- Facilidad de utilización e instalación
- Bajo coste de fabricación y adquisición
- Gran capacidad de transmisión de datos en redes de área local
- Rápida conectividad y actualizable
- Buena latencia en redes LAN

Uso

- En redes de área local Ethernet.
- Telefonía analógica.
- Telefonía digital.
- Terminales síncronos.
- Terminales asíncronos.
- Líneas de control y alarmas.

Fibra Óptica

A diferencia de las anteriores la fibra óptica no transporta información como señales eléctricas, sino que lo hace a través de variaciones de un haz de luz a través de una fibra de vidrio. La fibra óptica consiste en un conducto generalmente de fibra de vidrio o silicio que transmite impulsos luminosos normalmente emitidos por un láser o LED. Las fibras utilizadas en telecomunicación a largas distancias son siempre de vidrio; las de plásticos sólo son usadas en redes locales.

En el interior de la fibra óptica, el haz de luz se refleja contra las paredes en ángulos muy abiertos, así que prácticamente avanza por su centro. Esto permite transmitir las señales casi sin pérdida por largas distancias. La fibra óptica ha reemplazado a los cables de cobre por su costo/beneficio.

Las fibras ópticas se clasifican de acuerdo con el modo de propagación de los rayos de luz emitidos, dentro de ellas tenemos;

- **Monomodo:** En este tipo de fibra, los rayos de luz transmitidos por la fibra viajan linealmente. Se le considera como el modelo más fácil de fabricar.

- **Multimodo Graded index:** Este tipo de fibra es más costosa y tiene una capacidad realmente amplia.
- **Multimodo Step Index:** Esta es una entre las dos anteriores en cuanto a costo y capacidad.

Principales ventajas

- Transmisión de datos a alta velocidad.
- Mejor ancho de banda
- Evita interferencias
- Mejora la calidad del video y sonido.
- Mayor seguridad en la transmisión de datos.

Uso

En el área de telecomunicaciones tenemos:

- Transmisión de Voz y dato.
- Televisión Digital.
- Telefonía Digital.
- Internet.
- Centrales telefónicas entre ciudades y países.
- Sistema de seguridad.
- Telemetría.
- Administración remota.
- Entre otras.

Red Inalámbrica

Se define como redes inalámbricas a todas aquellas que transportan ondas electromagnéticas sin utilizar un conducto físico, sino que se transmiten por el aire. Este tipo de comunicación se denomina comunicación inalámbrica. Se lleva a cabo mediante antenas. Pueden ser de tipo direccional, donde las antenas (emisora/receptora) deben estar alineadas, omnidireccional donde se transmite en todas direcciones siendo así recibida por múltiples antenas.

Las transmisiones inalámbricas se pueden clasificar en:

- Onda de Radio
- Microondas
- Vía satélite

Medios de transmisión aéreas

Ondas de Radio

Son las más usadas, pero tienen apenas un rango de ancho de banda entre 3 KHz y los 300 GHz. Son poco precisas y solo son empleadas por determinadas redes de datos o los infrarrojos.

Se utilizan para establecer comunicaciones entre computadoras cercanas.

Las señales aéreas pueden viajar del origen al destino de formas diferentes: En superficie, por el cielo y en línea de visión.

- **Propagación por Superficie:** Las ondas de radio viajan a través de la porción más baja de la atmósfera, abrazando a la tierra. Las señales emanan en todas las direcciones desde la antena de transmisión. La distancia depende de la cantidad de potencia en la señal. Cuanto más grande es la potencia, más grande es la distancia.

- **Propagación por el cielo:** Las ondas de radio con una frecuencia mayor se irradian hacia arriba en la ionosfera y permite distancias mayores con una potencia de salida menor.

- **Propagación por la línea de Vista:** Se transmiten señales de muy alta frecuencia directamente de antena. La propagación por la línea de vista es truculenta porque las transmisiones de radio no se pueden enfocar completamente y deben ser direccionales.

Principales Ventajas

- Ahorro de costos, ya que no requiere una gran inversión.
- Aumento en la frecuencia y fiabilidad de la recopilación de los datos.
- Permiten el uso de diferentes protocolos sobre la misma capa de comunicaciones, dando al usuario una mayor flexibilidad.
- En cuanto a privacidad aportan una seguridad (para las industrias) siempre y cuando se cumplan ciertos requisitos.
- Versatilidad en lo que respecta al terreno de las comunicaciones en el caso que sea de difícil acceso en una zona.

Uso

Abarcan todos los dispositivos de comunicación que tenemos. Como:

- Televisión.
- Sistema GPS.
- Redes móviles.

Infrarrojo

Las redes por infrarrojos permiten la comunicación entre dos nodos, usando una serie de leds infrarrojos para ello. Se trata de emisores/receptores de las ondas infrarrojas entre ambos dispositivos, cada dispositivo necesita "ver" al otro para realizar la comunicación por ello es escasa su utilización a gran escala. Esa es su principal desventaja.

Bluetooth

Es una especificación industrial para redes inalámbricas de área personal (WPANs) que posibilita la transmisión de voz y datos entre diferentes dispositivos mediante un enlace por radiofrecuencia. Los principales objetivos que se pretende facilitar las comunicaciones entre equipos móviles y fijos, eliminar cables y conectores entre éstos y ofrecer la posibilidad de crear pequeñas redes inalámbricas y facilitar la sincronización de datos entre equipos personales.

Wimax

(Worldwide Interoperability for Microwave Access o Interoperabilidad para el Accesso a Microondas) es una forma de transmisión de datos usando microondas de radio. Esta tecnología es usada comúnmente para Internet inalámbrica de banda ancha dentro de un área geográfica determinada. El protocolo que caracteriza a esta tecnología es el 802.16.
Esta es una tecnología inalámbrica al igual que el Wi-Fi pero con la diferencia de que WiFi es solo para crear redes inalámbricas locales obteniendo el servicio a través de un cable mediante un módem. Pero WiMAX obtiene el servicio de manera inalámbrica y la cobertura es amplia.

Principales Ventajas

- Rapidez y sencillez de la instalación
- Facilidad de funcionamiento y movilidad: podemos conectarnos desde cualquier sitio donde llegue la cobertura sin mayor problema.
- Gran escalabilidad: permite el uso simultáneo de múltiples usuarios de manera simultánea.
- No requiere tener fijo en casa ni instalación
- No suele tener gastos de instalación
- Buena seguridad: suele contar con grandes medidas de seguridad, cifrado de información, etc.
- VoIP: WiMAX proporciona varios servicios añadidos como el uso de llamadas VoIP.
- Conexión a Internet en sitios donde otras tecnologías puede que no lleguen.

Wireless

(Inalámbrico o sin cables) es un término usado para describir las telecomunicaciones en las cuales las ondas electromagnéticas (en vez de cables) llevan la señal sobre parte o toda la trayectoria de la comunicación. Algunos dispositivos de monitorización, tales como alarmas, emplean ondas acústicas a frecuencias superiores a la gama de audiencia humana; éstos también se clasifican a

veces como Wireless. Los primeros transmisores sin cables vieron la luz a principios del siglo XX usando la radiotelegrafía (código Morse). Más adelante, como la modulación permitió transmitir voces y música a través de la radio, el medio se llamó radio. Con la aparición de la televisión, el fax, la comunicación de datos, y el uso más eficaz de una porción más grande del espectro, se ha resucitado el término Wireless.

Ejemplos comunes de equipos Wireless:

- Teléfonos móviles, que permiten colectividad entre personas.
- El sistema de posicionamiento global (GPS), que permite que coches, barcos y aviones comprueben su localización en cualquier parte de la tierra.
- Periféricos de ordenador Wireless, como el ratón, los teclados y las impresoras, que se pueden también conectar a un ordenador vía Wireless.
- Teléfonos inalámbricos, de más corto alcance que los teléfonos móviles.
- Mandos a distancia (para televisión, vídeo, puertas de garaje, etc.) y algunos sistemas de alta fidelidad.
- Monitores para bebés, estos dispositivos son unidades de radio simplificadas que transmiten/reciben dentro de una gama limitada.
- Televisión vía satélite, permiten que los espectadores, desde casi cualquier parte, seleccionen entre centenares de canales.
- LANS Wireless o local área networks, proporcionan flexibilidad y fiabilidad para usuarios de ordenadores.

Microondas Terrestre

Las microondas están definidas como un tipo de onda electromagnética situada en el intervalo del milímetro al metro.

Este sistema, se utiliza en tierra para comunicar sitios separados por accidentes geográficos que hacen poco práctica y costosa la instalación de un medio físico. La condición principal para realizar una conexión de microondas es la existencia de lo que se denomina una línea de vista física entre las antenas emisora y receptora. La distancia máxima de enlace que se logra sin problemas de atenuación y "Fading" de la señal es de aproximadamente 50 Km. La conexión de microondas sufre alteraciones cuando encuentra obstáculos físicos y se afecta con las condiciones del clima.

Las microondas están definidas como un tipo de onda electromagnética situada en el intervalo del milímetro al metro y cuya propagación puede efectuarse por el interior de tubos metálicos. Es en si una onda de corta longitud. Tiene como características que su ancho de banda varía entre 300 a 3.000 MHz, aunque con algunos canales de banda superior, entre 3´5 GHz y 26 GHz. Es usado como enlace entre una empresa y un centro que funcione como centro de conmutación del operador, o como un enlace entre redes LAN.

Para la comunicación se deben usar antenas parabólicas, las cuales deben estar alineadas o tener visión directa entre ellas, además entre mayor sea la altura mayor el alcance, sus problemas se

dan perdidas de datos por atenuación e interferencias, y es muy sensible a las malas condiciones atmosféricas.

Uso

- Difusión de televisión.
- Transmisión telefónica a larga distancia.
- Redes privadas.

Principales Ventajas

- Sin necesidad de cables
- Múltiples canales disponibles
- Amplio ancho de banda
- Es capaz de transmitir grandes cantidades de datos
- Sujeto a las interferencias electromagnéticas
- Costos relativamente bajos

Vía Satélite (Microondas Aéreo)

Conocidas como microondas por satélite, está basado en la comunicación llevada a cabo a través de estos dispositivos, los cuales después de ser lanzados de la tierra y ubicarse en la órbita terrestre, realizan la transmisión de todo tipo de datos, imágenes, etc., según el fin con que se han creado. Las microondas por satélite manejan un ancho de banda entre los 3 y los 30 GHz, y son usados para sistemas de televisión, transmisión telefónica a larga distancia y punto a punto y redes privadas punto a punto. Las microondas por satélite, o mejor, el satélite en si no procesan información, sino que actúa como un repetidor-amplificador y puede cubrir un amplio espacio de espectro terrestre.

Uso

- Difusión de televisión.
- Telefonía a larga distancia.
- Redes privadas

Principales Ventajas

- Comunicaciones sin cables, independientes de la localización
- Amplitud de cobertura
- Gran ancho de banda • Seguridad de la señal
- Su área de cobertura es muy superior al de una señal terrestre

- Su costo es independiente de la distancia desde el centro de la zona de cobertura.
- Instalación rápida de una red
- Servicio total proporcionado por un único proveedor

REDES DE ACUERDO CON SU DISTRIBUCIÓN GEOGRÁFICA

La industria de las computadoras ha avanzado en muy corto tiempo. El hecho de que una sola computadora sea la que satisfaga todas las necesidades de cálculos de una organización, está siendo reemplazada por varias computadoras separadas pero interconectadas entre sí efectuando el mismo trabajo, pero con más fiabilidad y respaldo en el momento de contar con fuentes alternativas de suministro y con la posibilidad de compartir recursos, programas e información a la distancia, ejecutar procesos en otro ordenador o acceder a sus ficheros y/o enviar mensajes. Esto es lo que se denomina en informática una red de computadoras.

Las terminales suelen estar conectados entre sí por cables. Pero si la red abarca una zona extensa, las conexiones pueden realizarse a través de líneas telefónicas, microondas, líneas de fibra óptica e incluso satélites.

Existe un factor muy importante para tener en cuenta al momento de instalar una red de computadoras y éste es, como mencionamos antes, su alcance o área de cobertura. Cada red en esta clasificación posee una estructura particular, ventajas y desventajas dependiendo de la funcionalidad final que se desee. A continuación, analizaremos cada una de estas redes, lo que otorgará al finalizar, una mayor capacidad para identificarlas en sus distintos usos.

CLASIFICACION DE REDES POR ALCANCE DISTRIBUCIÓN GEOGRÁFICA

Las redes, ya sea por cable estructurado o por medio inalámbrico pueden ser faccionada de acuerdo con su alcance o cobertura. Notoriamente cuando mayor sea el espacio que necesitamos cubrir, será más complicado y costosa la instalación de cables entre otros, por ello existen distintos tipos de redes informáticas de acorde a su alcance. Ellas son:

PAN: Red de área personal.

Cuando nombramos pan, estamos hablando de una red informática de pocos metros, semejante a la distancia que se necesita para intercambiar datos por vía buetooth. Esta red sirve para conectar pocos dispositivos cercanos conectados de alguna manera entre sí, por ejemplo (teléfono, laptop, impresora, pc) entre otros, existe la posibilidad de poder aumentar el radio de cobertura y evitar una instalación de cableado, para que sea posible es necesario obtener un router, y con ello la cobertura aumentaría entre 10 a 25 metros.

LAN: Red de área local.

La red de área local es una red informática que generalmente es utilizada en la mayoría de las empresas. Abarca desde un pequeño local hasta un edificio completo, esta red permite conectar diferentes periféricos entre si (impresora, escáneres etc.) para que estos puedan intercambiar datos y ordenes desde los diferentes extremos del edificio o lugar. Este tipo de red puede comprender desde los 200mts hasta 1km de cobertura.

MAN: Red de área metropolitana.

Este tipo de red es mucho más amplia que las nombrada anteriormente, La red de área metropolitana abarca espacios metropolitanos muy grandes, suelen utilizarse cuando las administraciones publicas deciden crear zonas wifi en grandes espacios además utilizan toda una infraestructura de cables de un operador de telecomunicaciones para el despliegue de redes de fibra óptica. Una red de esta magnitud puede conectar diferentes LAN que hay en un espacio de alrededor de 50 kilómetros.

WAN: Red de área amplia.

Son las que suelen desplegar las empresas proveedoras de Internet para cubrir las tipos de casino necesidades de conexión de redes de una zona muy amplia, como una ciudad o país.

SAN: Red de área de almacenamiento

Es una red propia para las empresas que trabajan con servidores y no quieren perder rendimiento en el tráfico de usuario, ya que manejan una enorme cantidad de datos. Suelen utilizarlo mucho las empresas tecnológicas.

VLAN: Red de área local virtual.
Las redes de las que hablamos normalmente se conectan de forma física. Las redes VLAN se encadenan de forma lógica (mediante protocolos, puertos, etc.), reduciendo el tráfico de red y mejorando la seguridad. Si una empresa tiene varios departamentos y quieres que funcionen con una red separada, la red VLAN.

A continuación, profundizaremos en algunas de estas redes mencionadas.

REDES DE AREA LOCAL

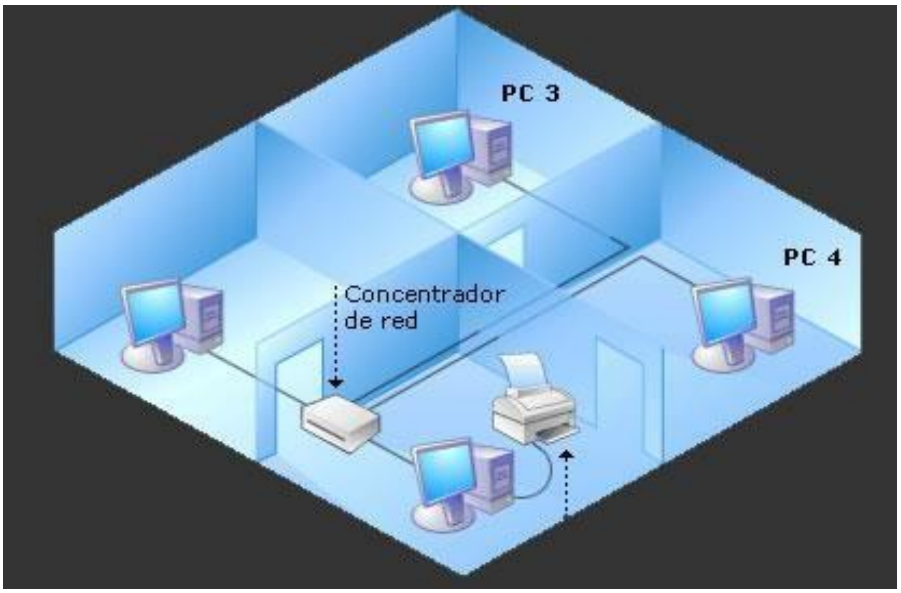
LAN (Local área Network)

Una red de área local, red local o LAN (del inglés local área network) es la interconexión de varias Computadoras y Periféricos. Su extensión está limitada físicamente a un edificio o a un entorno de 200 metros, o con Repetidores podría llegar a la distancia de un campo de 1 kilómetro. Su aplicación más extendida es la interconexión de computadoras personales y estaciones de trabajo en oficinas, fábricas, etc., para compartir recursos e intercambiar Datos y Aplicaciones. En definitiva, permite una conexión entre dos o más equipos.

El término red local incluye tanto el Hardware como el Software necesario para la interconexión de los distintos dispositivos y el tratamiento de la información

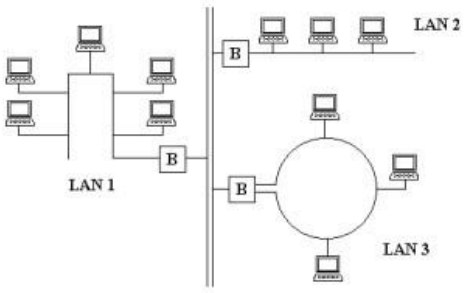
Características principales de las LAN

1. Tecnología Broadcast (difusión) con el medio de transmisión compartido.
2. Capacidad de transmisión comprendida entre 1 Mbps y 1 Gbps.
3. Extensión máxima no superior a 3 km
4. Uso de un medio de comunicación privado
5. La simplicidad del medio de transmisión que utiliza (Cable coaxial, Cables telefónicos y Fibra óptica)
6. La facilidad con que se pueden efectuar cambios en el Hardware y el Software
7. Gran variedad y número de dispositivos conectados
8. Posibilidad de conexión con otras redes
9. Limitante de 100 m, puede llegar a más si se usan Repetidores.



Ventajas

Por ejemplo en una empresa permite compartir Bases de datos (se elimina la redundancia de datos), Programas (se elimina la redundancia de Software); poniendo a nuestra disposición otros medios de comunicación como pueden ser el Correo electrónico y el Chat. Nos permite realizar un proceso distribuido, es decir, las tareas se pueden repartir en distintos nodos y nos permite la integración de los procesos y datos de cada uno de los Usuarios en un sistema de trabajo corporativo. Tener la posibilidad de centralizar información o procedimientos facilita la administración y la gestión de los equipos. Además, una red de área local conlleva un importante ahorro, tanto de tiempo, ya que se logra gestión de la información y del trabajo, como de dinero, ya que no es preciso comprar muchos periféricos se consume menos papel, y en una conexión a Internet se puede utilizar una única conexión telefónica o de Banda Ancha compartida por varias terminales conectadas en Red.



Redes LAN en una empresa

REDES DE AREA AMPLIA

Una red de área amplia (Wide Área Network, o WAN) se denomina a las conexiones informáticas de mayor envergadura, es decir, las más abarcativas y de mayor velocidad, que cubren una extensa porción geográfica del planeta. Las redes WAN incorporan diversas redes de menor tamaño en una sola (redes de área local LAN o no), interconectando así usuarios separados por enormes distancias, con mayores tasas de transmisión y con diversos niveles (capas) de datos.

Esto implica la necesidad de máquinas dedicadas por completo a la ejecución de programas de usuario (hosts), la presencia de aparatos enrutadores y conmutadores, o la utilización de máscaras de subred para conectar varios hosts.

Existen redes públicas que son operadas por proveedores de servicios de Internet para permitir a sus clientes el acceso a este, y redes privadas de área amplia que son utilizadas principalmente por empresas, por ejemplo, para permitir servicios en la nube y para conectar las redes de las diferentes sedes de la empresa.

Una red privada virtual (VPN) facilita la conectividad entre sitios WAN. Este es un software que da acceso al usuario al WAN, pero hay que asegurarse de que las acciones empresariales sigan siendo confidenciales. La comunicación que se da dentro de un contexto de RPV está encriptada y, por lo tanto, no está visible para terceros. Al igual que en una intranet, los usuarios deben iniciar sesión con un código. Esto hace que se le garantice o rechace el acceso a los usuarios.

Los enlaces directos de fibra óptica también se utilizan para conectar sitios en una WAN –y casi siempre ofrecen mayor rendimiento, fiabilidad y seguridad que las VPN, pero son prohibitivos para que la mayoría de las empresas las adquieran y operen. Estos son especialmente adecuados para conexiones a larga distancia sobre tierra y agua. Los avances más recientes son las vías de transmisión de datos de banda ancha por satélite, que se pueden establecer con relativa rapidez. En la práctica, se suele utilizar una combinación de varios medios de transmisión distintos. Con los llamados convertidores de medios, se pueden interconectar distintos tipos de cables. En los grandes nodos de Internet hay puntos de intercambio especiales interconectados, donde a menudo hay más de cien redes interconectadas para permitir un intercambio de datos eficiente. Los repetidores se encargan de que los paquetes de datos no pierdan información, incluso a grandes distancias.

Las WAN sobre las conexiones de red cableadas siguen siendo el medio preferido para la mayoría de las empresas, la forma más estable y rápida de intercambiar información (a larga distancia). Sin embargo, la desventaja de este sistema es el mantenimiento. Sobre todo, cuando la comunicación se produce con otros continentes. Por ejemplo, el mantenimiento de los cables en el fondo del océano implica altos costes.

En una empresa, un ejemplo de WAN puede consistir en conexiones al corporativo, sucursales, instalaciones de colocación, servicios en la nube y otras instalaciones. Normalmente, se utiliza un enrutador u otro dispositivo multifunción para conectar una LAN a una WAN. Las WAN corporativas permiten a los usuarios compartir el acceso a aplicaciones, servicios y otros recursos ubicados centralmente. Esto elimina la necesidad de instalar el mismo servidor de aplicaciones, firewall u otro recurso en múltiples ubicaciones, por ejemplo.

Tipos de red WAN

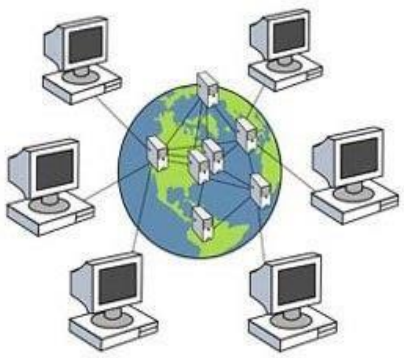
Las redes WAN pueden ser de distinto tipo, por ejemplo:

- Red WAN por circuitos. Se trata de redes de discado telefónico, que reciben la dedicación plena del ancho de banda mientras se emplea la línea telefónica, pero son lentas y ocupan la línea telefónica.

- Red WAN por mensaje. Se compone de ordenadores (conmutadores) que aceptan el tráfico de cada una de las terminales de la red y administran el flujo de la información mediante mensajes (e información en la cabecera de los mismos) que pueden ser borrados, redirigidos o respondidos automáticamente.

- Red WAN por paquetes. La información en estos casos es fraccionada en partes pequeñas (paquetes) y una vez que llegan a su destino son nuevamente integradas en el mensaje original.

Un perfecto ejemplo de red WAN es la Internet, también conocida como World Wide Web (Red de Alcance Mundial), que permite la conexión a un conjunto enorme de datos disponibles en línea, desde cualquier parte del mundo que cuente con un punto de acceso y un ISP (Internet Service Provider, “Proveedor de Servicios de Internet”). Lo mismo ocurre con las redes bancarias nacionales, que administran información financiera secreta, o con las redes de televisión por suscripción, que emplean satélites y otros mecanismos para emitir señal paga a los hogares suscritos.



RED DEDICADA

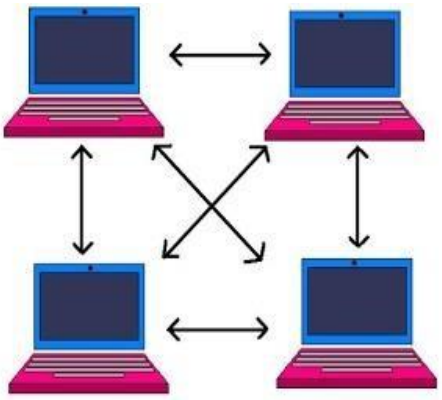
Se trata de una red que tiene asignados ciertos recursos de manera permanente y única, esto es por medio de infraestructura o de manera lógica, por lo que solamente un cliente tiene acceso a los beneficios contratados. Normalmente, se utilizan para garantizar la disponibilidad de una cierta capacidad de transporte en ciertas condiciones a grandes usuarios de comunicaciones.

Las tecnologías que soportan estas redes dedicadas dependen, en primer lugar, del tipo de información considerado: voz, vídeo (junto con audio) o datos. También se utilizan las mismas redes de transporte para cualquier otra comunicación a las que se incorporan los mecanismos adecuados para separar y priorizar el tráfico en cuestión.

Variantes

Redes punto a punto:

Son aquellas redes que responden a un tipo de arquitectura de red en las que cada canal de datos se usa para comunicar únicamente dos nodos, en contraposición a las redes multipunto, en las cuales cada canal de datos se puede usar para comunicarse con diversos nodos.



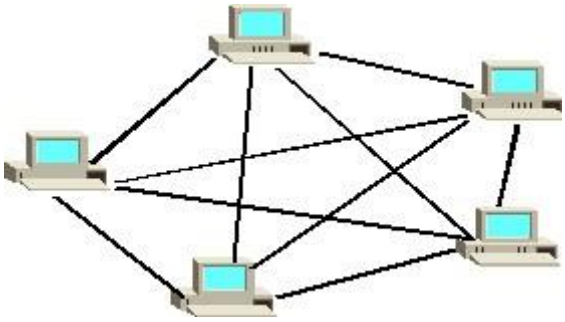
En una red punto a punto, los ordenadores funcionan tanto como receptores como emisores de información.

Las principales ventajas de este tipo de redes son su facilidad a la hora de ser configuradas, su simplicidad y el poco costo ya que no requiere de otros dispositivos de red.

Redes multipunto:

Las redes multipunto son redes en las cuales cada canal de datos se puede utilizar para comunicarse con diversos nodos.

Este tipo de redes se caracterizan por permitir la unión de varios terminales a su correspondiente computadora compartiendo solo una línea de transmisión, es decir, solo existe una línea de comunicación cuyo uso está compartido por todas las terminales en la red. La información fluye de forma bidireccional y es discernible para todas las terminales de la red.



Las ventajas de las redes multipunto son el abaratamiento de su costo, la transmisión de información en tiempo real y los enlaces de largas distancias.

Ventajas de una red dedicada

Las principales ventajas de una red dedicada son:

- Brindan privacidad a la información.
- La velocidad de subida y bajada es simétrica y estable.
- No hay límite de volumen de carga o descarga.
- Su instalación se realiza en días.
- El servicio está monitoreado las 24 horas del día.

Desventajas de una red dedicada

Algunas de las desventajas de las redes dedicadas son:

- Su costo mensual es relativamente muy costoso.
- Con este tipo de líneas todas las áreas no están cableadas.
- En cada punto que se requiera conectar se necesita una línea privada

RED DE AREA METROPOLITANA

Una red de área metropolitana (Metropolitan Área Network o MAN) es una red de comunicaciones de alta velocidad (banda ancha) que da cobertura en un área geográfica limitada como una ciudad, suburbio o área metropolitana. Proporciona capacidad de integración de múltiples servicios mediante la transmisión de datos, voz y video, sobre medios de transmisión como fibra óptica y par trenzado (MAN BUCLE). Las redes MAN BUCLE ofrecen velocidades de 10 Mbit/s o 20 Mbit/s sobre pares de cobre y 100 Mbit/s y 1 Gbit/s y 10 Gbit/s mediante fibra óptica.

Una MAN utiliza tecnologías como ATM, Frame Relay, DSL (Digital Suscriber Line), WDM (Wavelenght Division Multiplexing), ISDN, E1/T1, PPP, etc. Para conectividad a través de medios de comunicación como cobre, fibra óptica y microondas.

El concepto de red de área metropolitana representa una evolución del concepto de red de área local a un ámbito más amplio, cubriendo áreas mayores que en algunos casos pueden llegar a una cobertura regional e incluso nacional mediante la interconexión de diferentes redes de área metropolitana.

Las redes de área metropolitana comprenden una ubicación geográfica determinada “ciudad, municipio” y su distancia de cobertura es mayor de 4 km. Son redes con dos buses unidireccionales, cada uno de ellos independiente del otro en cuanto a transferencia de datos.

MAN Pública y privada

Una red de área metropolitana puede ser pública o privada.

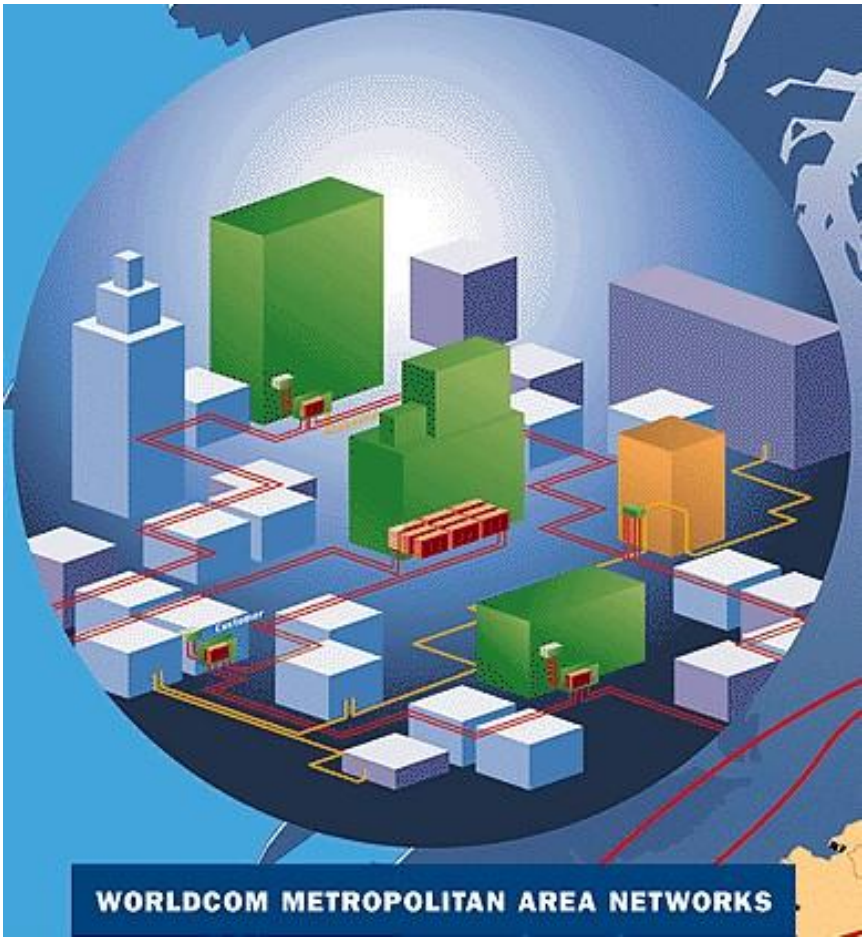
Una MAN privada podría ser un departamento o administración con edificios distribuidos por la ciudad, transportando todo el tráfico de voz y datos entre edificios por medio de su propia MAN y encaminando la información externa por medio de los operadores públicos.

Una MAN publica es la infraestructura que un operador de telecomunicaciones instala en una ciudad con el fin de ofrecer servicios de banda ancha a sus clientes localizados en esta área geográfica.

Características

- **Trafico en tiempo real:** Las redes de área metropolitana garantizan unos tiempos de acceso a la red mínimos, lo cual permite la inclusión de servicios síncronos necesarios para aplicaciones en tiempo real.

- **Alta fiabilidad:** Fiabilidad referida a la tasa de error de la red mientras se encuentra en operación. Se entiende por tasa de error el número de bits erróneos que se transmiten por la red
- **Alta Seguridad:** La fibra óptica ofrece un medio seguro porque no es posible leer o cambiar la señal óptica sin interrumpir físicamente el enlace.
- **Alta disponibilidad:** Disponibilidad referida al porcentaje de tiempo en el cual la red trabaja sin fallos. Las redes de área metropolitana tienen mecanismos automáticos de recuperación frente a fallos.



TOPOLOGIAS INALAMBRICAS

En informática, las redes inalámbricas son las conexiones entre nodos que se dan por medios de ondas electromagnéticas, sin necesidad de una red cableada o alámbrica. Los puertos son los capaces de llevar a cabo la transmisión y recepción de los datos.

Una característica favorable de este tipo de redes es la reducción de costos, ya que elimina el cableado y los medios físicos entre nodos. Por lo contrario, se debe aumentar su seguridad y control porque es más fácil de manipular para los intrusos.

Redes inalámbricas de Acuerdo con su Distribución Geografica

- **WPAN – Wireless Personal Area Network:** Son redes de cobertura personal. El alcance típico de las WPAN es alrededor de diez metros aproximadamente. La finalidad es comunicar cualquier dispositivo personal con sus periféricos, así como permitir una comunicación directa a corta distancia entre los mismos. Ejemplos de estas tecnologías: HomeRF, Bluetooth, ZigBee, RFID.
- **WLAN – Wireless Local Area Network:** Tecnologías basadas en WI-FI. Puede presentar mejoras con respecto a la velocidad de sus estándares y alcanza una distancia de hasta 20 km.
- **WMAN – Wireless Metropolitan Area Network:** Se utiliza para redes de área metropolitana basadas en WiMAX, un estándar de comunicación inalámbrica basado en la norma IEEE 802.16. WiMAX es un protocolo parecido a WI-FI, pero con más cobertura y ancho de banda. También podemos encontrar otros sistemas de comunicación con LMDS.
- **WWAN – Wireless Wide Area Network:** Una WWAN difiere de una WLAN en que usa tecnologías de red celular de comunicaciones móviles como WiMAX, UMTS, GPRS, EDGE, CDMA2000, GSM, CDPD, Mobitex, HSPA y 3G para transferir los datos. También incluye LMDS y Wi-Fi autónoma para conectar a internet.

Aplicaciones

- Las redes más importantes con aplicaciones inalámbricas, del rango de frecuencias que abarcan las ondas de radio, son la VLF, LF, MF, HF, VHF, UHF.
- Las microondas por satélite se usan para la difusión de televisión por satélite, transmisión telefónica a larga distancia y en redes privadas, por ejemplo.
- Mediante las microondas terrestres, existen diferentes aplicaciones basadas en protocolos como Bluetooth o ZigBee para interconectar ordenadores portátiles, PDAs, teléfonos u otros aparatos. También se utilizan las microondas para comunicaciones con radares.
- Los infrarrojos tienen aplicaciones como la comunicación a corta distancia de los ordenadores con sus periféricos.
- Las ondas de radio deben confinarse tanto como sea posible, pero es difícil de conseguir totalmente. Se emplean antenas direccionales y se configura la potencia de transmisión de los puntos de acceso para un buen trabajo.

Seguridad

- Debe existir algún mecanismo de autenticación de doble vía, que permita al cliente verificar que se está conectando a la red correcta, y a la red constatar que el cliente está autorizado para acceder a ella.
- Se deben cifrar los datos cuando viajan por aire para evitar que equipos intrusos a la red puedan capturar datos.

OTROS TIPOS

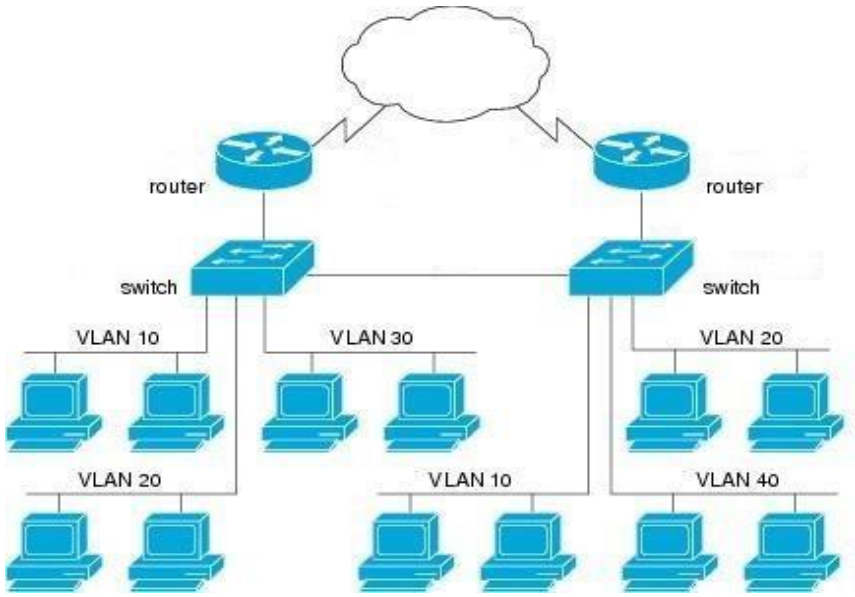
Redes VLAN (Virtual Local Area Network – Red de Área Local Virtual)

Una virtual LAN es un método que permite crear redes lógicas e independientes dentro de una misma red física mayor. Cada una de estas redes virtuales se conectan a un switch que, a su vez, va conectado a la red principal. Cada VLAN cuenta con su propio dominio de difusión, o dominio de broadcast, lo que hace que los mensajes enviados solo sean recibidos por los participantes de ese dominio.

Dependiendo de la configuración que posea, una VLAN puede calificarse de diferentes maneras:

- VLAN basada en puertos: También conocida como port switching es una configuración donde se especifica que puertos del switch pertenecen a cada VLAN, y los miembros de esa red son los que se conectan a ese puerto. En caso de que un usuario se cambia de puerto físicamente, habría que reconfigurar la red.
- VLAN basada en direcciones MAC: Es una configuración similar a la anterior, salvo que, en lugar de asignarse a nivel puerto, se hace con la dirección MAC del dispositivo. La principal ventaja de esta configuración es que no es necesario reconfigurar el dispositivo de conmutación cuando un usuario cambia su localización. Y el mayor inconveniente es que se debe asignar a los usuarios uno por uno.
- VLAN basada en tipo de protocolo: Este tipo de configuración permite crear una red virtual por cada tipo de protocolo (IPv4, IPv6, AppleTalk, IPX, etc.), por lo que se agruparían todos los equipos que utilicen el mismo protocolo en la misma red.
- VLAN de niveles superiores: También llamada VLAN de aplicaciones, es una configuración que crea una red virtual en función de la aplicación para la que será utilizada. Para esta red intervienen distintos factores, como puertos, direcciones MAC, subredes, hora del día, forma de acceso, conficiones de seguridad del equipo, etc.

El hecho de que se pueda definir una nueva red por encima de la red física ofrece diversas ventajas: como principal, la flexibilidad en la administración y en los cambios de la red es mayor, dado que el administrador de la red puede asignar una misma computadora a diferentes redes virtuales en distintos momentos. Puesto que la información está limitada a un número pequeño de estaciones pertenecientes a cada dominio, la seguridad es mayor. De igual manera funciona con el rendimiento, ya que los paquetes no tienen que atravesar toda la red para llegar a su destino, únicamente una muy pequeña parte de ella.



Redes PAN (Personal Área Network – Red de Área Personal)

Una red PAN, es utilizada para interconectar dispositivos centrados en el espacio de trabajo de una persona. Proporciona transmisión de datos entre dispositivos como computadoras personales, periféricos inalámbricos, smartphones, tablets, controles remotos, etc. Existen dos tipos de redes PAN, las alámbricas y las inalámbricas, y de esto depende su cobertura. Las alámbricas suelen tener un alcance de 10 metros, y el cable con el que se conectan tiene una terminación USB, mientras que las inalámbricas, también conocidas como WPAN (Wireless Personal Area Network), alcanzan los 25 metros. Estas últimas son las más comunes, y se basan en las tecnologías Bluetooth, Wireless USB, IrDA, ZigBee o Z-Wave, entre otras, para su funcionamiento.

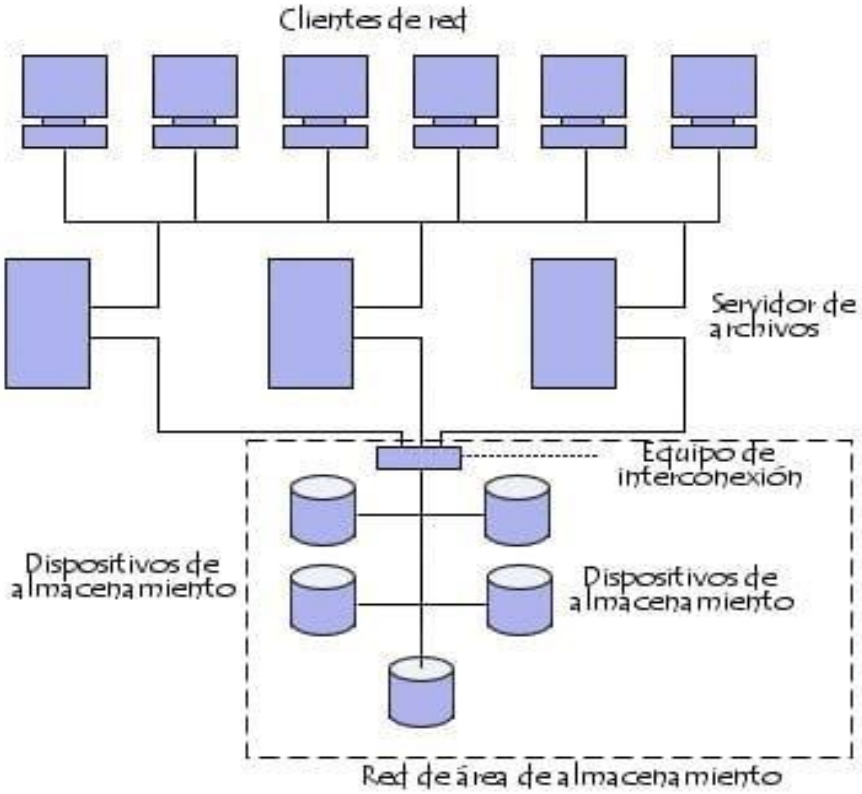
Además de establecer la conexión entre cada uno de los dispositivos, las redes PAN permiten la conexión con otras redes de mayor tamaño, esto se denomina uplink (Enlace de subida).

Las PAN, son redes económicas, seguras y fáciles de usar. No es necesario un cableado previo, por lo que no se generan gastos en ese ámbito; todos los dispositivos requieren de autorización para conectarse, lo que las hace seguras; y no precisan de una configuración avanzada. Sin embargo, la transferencia de datos mediante este tipo de red suele ser más lenta en comparación a otras.

Redes SAN (Storage Área Network – Red de Área de Almacenamiento)

SAN es una red de almacenamiento dedicada de alta velocidad que brinda acceso al almacenamiento en bloque. Este tipo de red se utiliza a nivel empresarial, y permite asignar y administrar de forma más fácil los recursos de almacenamiento, logrando una mayor eficiencia. Además, el almacenar los datos de forma centralizada, permite a las organizaciones implementar metodologías uniformes en temas de seguridad, protección y recuperación de datos.

El rendimiento y capacidad de este tipo de redes es extremadamente amplio, llegando a tener un almacenamiento de miles de terabytes y una velocidad aproximada de 100 megabytes por segundo.



Este tipo de redes están compuestas por tres capas:

- La capa de host: Consiste principalmente en los servidores, componentes y software (Sistemas operativos).
- La capa de fibra: La cual está compuesta por los cables de fibra óptica, los hubs y switches que conforman el punto central de la conexión.
- La capa de almacenamiento: Es en donde se encuentran las formaciones de discos y cintas utilizados para almacenar los datos.

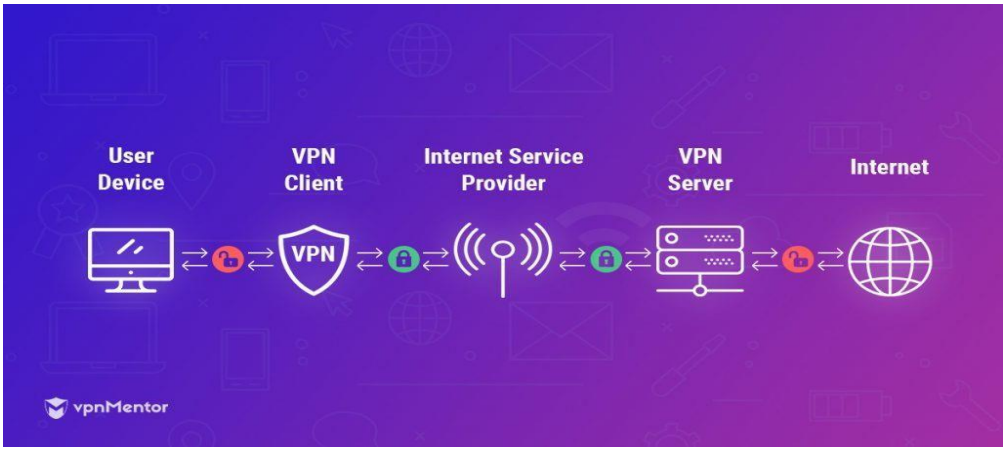
Ventajas:

- Este tipo de redes tienden a maximizar el rendimiento, puesto que las rutas de almacenamiento son muchas, ya que un servidor puede acceder a uno o varios discos y un disco puede ser accedido por varios servidores.
- Tiene la capacidad de respaldar o ser respaldada en localizaciones físicamente distantes, dado que el objetivo de estas redes es perder el menor tiempo posible.
- Posee una alta disponibilidad de los datos.
- Las SAN tienen compatibilidad con dispositivos SCSI (Small Computer System Interface), lo que permite el crecimiento de la red a partid de hardware ya existente.
- El rendimiento está directamente relacionado con el tipo de red que se utiliza para su armado. En caso de usar un canal de fibra óptica, el ancho de banda se extiende hasta un aproximado de 100 MBps. Esto se aplica de igual manera a su capacidad, ya que se puede extender de manera casi ilimitada, llegando a tener una capacidad de miles de terabytes.

La mayor desventaja a la hora de instalar una red de almacenamiento es su costo, dado que para poder formar una red de gran tamaño se debe de invertir mucho dinero.

*Redes VPN (*Red privada Virtual)

Es una tecnología de red que se utiliza para conectar una o más computadoras a una red privada utilizando Internet. Ofrece un mayor nivel de protección y privacidad al navegar por Internet.



¿Cómo funciona?

Se obtiene una dirección IP diferente a tu IP real, por lo que tu identidad en Internet está a salvo en todo momento**.** Tu destino no sabe que tu tráfico viene de tu ubicación real ya que, en realidad, llega a éste desde el servidor VPN.

Es decir que: tu VPN es el intermediario que has contratado para asegurarte de que tus datos están protegidos desde que van desde ti hasta la web o servicio que visitas Una VPN también te da privacidad al mantener ocultos tu IP real, dispositivo y ubicación (aunque son visibles para tu proveedor de VPN).

Para los demás usuarios, tu ubicación es la de tu servidor VPN, y tu dirección IP la que éste te proporciona, la cual comparten potencialmente miles de estos usuarios.

Ventajas

- Mayor nivel de anonimato
- Podes evitar la censura
- Podes descargar torrents de forma segura
- Mejor conexión a internet
- Podes conectarte desde cualquier dispositivo

Protocolos En Red

¿Qué es un protocolo de red?

Parecería que para integrar un equipo a una red de ordenadores bastaría con interconectarlos entre sí con ayuda de un cable de LAN, pero los sistemas informáticos no tienen la capacidad de intercambiar paquetes de datos sin ayuda, y no pueden, por ello, **establecer ninguna conexión de datos**. Esta tarea le corresponde a los protocolos de red, que, en conjunto con sus respectivas familias de protocolo, actúan en la llamada capa de mediación o de red, el nivel 3 en el modelo OSI y establecen una serie de acuerdos para el intercambio de datos, regulando, así, las condiciones para el transporte, el direccionamiento, el enrutamiento (camino del paquete) y el control de fallos. Esto significa que, para que dos ordenadores se puedan comunicar entre sí, han de utilizar los mismos protocolos de red, de forma que acuerdan las mismas **condiciones para la transmisión**, que se añaden al paquete en el encabezado o como anexo:

- Tamaño del paquete o de los paquetes de datos
- Tipo de paquete
- Emisor y destinatario
- Otros protocolos implicados

¿Por qué existen diferentes protocolos de red?

No todas las conexiones de datos entre sistemas de ordenadores están cortadas por el mismo patrón. No es lo mismo interconectar dos ordenadores en una red doméstica que conectar un ordenador a Internet, formando parte de una unión gigantesca de computadoras y enviando datos a varios destinatarios. De igual forma, las jerarquías de los participantes también juegan un papel destacado en la comunicación, lo que origina que se den **distintos protocolos de red para cada una de las formas de comunicación**, diferenciados entre sí en función de los siguientes aspectos y escenarios posibles de aplicación:

1. **Número de participantes en la comunicación**: los protocolos de red se diferencian por el número de ordenadores que puede participar de la conexión. Si los datos que se transmiten solo tienen un destinatario, esta transferencia se conoce como **unicast**, si el intercambio se produce entre dos o más sistemas se habla entonces de conexiones **multicast**, y si el envío de paquetes de datos implica a todos los participantes se denomina **broadcasting**, un tipo de conexión típico de la emisión de radio y de televisión.

2. **Modo de transmisión de los datos**: la dirección en la que circulan los datos también permite diferenciar los protocolos de red entre sí. Los protocolos con transferencia **símplex** (sx) o unidireccional solo admiten la comunicación unilateral, en la cual un ordenador funciona únicamente como emisor y el otro como receptor, en la transmisión **semi-dúplex** (half-duplex,

hdx) ambos ordenadores intercambian los roles de emisor y receptor pero no simultáneamente y, por último, el modo **dúplex completo** (full-duplex, fdx) permite el envío de datos en ambas direcciones simultáneamente.

3. **Jerarquía de los participantes**: ciertos tipos de conexión como el modelo cliente-servidor se basan en unas estructuras jerárquicas claramente definidas. En este caso concreto varios clientes pueden iniciar la conexión con un único servidor, el cual procesa las solicitudes. La forma opuesta de esta **comunicación asimétrica** la constituye la simétrica, también denominada red entre iguales o peer to peer. En esta conexión todos los ordenadores están en igualdad de condiciones y pueden proporcionar servicios y utilizarlos.

4. **Sincronización de la comunicación**: la transmisión de datos también se puede diferenciar en función de si se sincronizan los bits entre emisor y receptor (comunicación síncrona) o no (comunicación asíncrona).

5. **Tipo de conexión**: por último, los protocolos de red se pueden dividir en aquellos orientados a la conexión y aquellos que no lo están. Los primeros requieren una conexión entre emisor y receptor durante la transmisión e intentan garantizar que los paquetes lleguen a su destino **en un orden determinado** y que, en caso de entrega fallida, se envíen nuevamente. Los segundos **no establecen ni interrumpen una conexión**, por lo que los paquetes que se envían contienen bastante menos información adicional, aunque pueden llegar en una secuencia arbitraria al destinatario y no se vuelven a enviar en caso de una transmisión fallida.

Aparte de las consideraciones de índole técnica, la gran **diversidad de protocolos de red** existente resulta, asimismo, de que muchos fabricantes desarrollaron en el pasado sus propios protocolos para sus dispositivos.

¿Cuántos protocolos de red existen?

Para la capa de red, de la misma forma que para el resto de las capas, también se da una serie de protocolos estandarizados y propietarios, indicados para diversos ámbitos de aplicación y en parte restringidos a ciertos sistemas operativos y dispositivos, algunos ya, incluso, obsoletos. Muchos de estos protocolos de red ya no se usan a día de hoy, como consecuencia, sobre todo, de la creciente expansión de la **familia de protocolos de Internet**, un conjunto de más de 500 protocolos entre los que también se incluye el más importante y popular protocolo de red **IP o Internet Protocol**, que constituye el fundamento de Internet.

El protocolo de Internet tiene la misión de **transportar los paquetes de datos de un emisor a un receptor a través de varias redes**. Con esta finalidad, este protocolo fija las directrices de direccionamiento y de enrutamiento, es decir, del itinerario que han de seguir los paquetes de datos.

IP no es solo el protocolo de red estándar para redes WAN (Wide Area Network), las únicas redes globales que interconectan Internet, sino también **para redes locales**. Todos los fabricantes y sistemas operativos soportan el protocolo de Internet, aunque presupone contar con la experiencia técnica necesaria en configuración, así como con el hardware (router) adecuado.

La siguiente tabla muestra una visión general de los protocolos de red históricamente más relevantes:

Los protocolos de transmisión de los paquetes de datos

Una vez establecida la base de la comunicación por parte de los protocolos de la capa de enlace, se requieren otros protocolos que permitan que los paquetes de datos lleguen a las aplicaciones correspondientes. Partiendo del modelo OSI, **este proceso se lleva a cabo en la capa de transporte** o capa 4. Para ello, cada pila posee también sus propios protocolos. Para la familia de protocolos de Internet estos son, en especial:

- **TCP** (Transmission Control Protocol) o protocolo de control de la transmisión
- **UDP** (*User Datagram Protocol*) o protocolo del datagrama del usuario

TCP, al igual que IP, también es considerado el estándar para las conexiones de red, por lo menos desde el gran éxito de Internet, y, en la mayoría de los casos, se construye sobre IP directamente, lo que origina que se hable a menudo de redes TCP/IP. Como protocolo orientado a la conexión, **TCP presupone una conexión** existente entre los participantes para poder transportar el paquete de datos, garantizando la transmisión fiable de los datos en tanto que los paquetes llegan íntegros y en el orden correcto al destinatario. Para hacer esto posible, el protocolo añade a los paquetes de datos información adicional como un **número de secuencia** o una **suma de verificación** (checksum), además de otro tipo de datos.

UDP es su equivalente en la familia de protocolos de Internet para la **transmisión simple y rápida de paquetes pequeños sin conexión**. Aunque las conexiones UDP no garantizan que el paquete llegue a su destinatario, la reducción de los datos de gestión (información adicional en el encabezado) otorga una mayor velocidad a aquellas transferencias de datos en las cuales se pueda tolerar algún error de transmisión. Es por este motivo que UDP se utiliza en el streaming de vídeo y audio, en peticiones al DNS, así como en conexiones VPN (Virtual Private Network).

Como la familia de protocolos de Internet, hay otras pilas de protocolo que también cuentan con protocolos de transmisión específicos construidos sobre sus protocolos de red y que, en gran parte, se asemejan mucho a TCP. Las redes Novell, por ejemplo, ofrecen el protocolo SPX en la capa de transporte. En el caso de la pila de AppleTalk, la transmisión de los paquetes tiene lugar con ayuda del ATP (AppleTalk Transaction Protocol).

Modelo OSI-ISO

El Open Systems Interconnection Model, conocido como modelo OSI por su abreviatura, fue creado por la Organización Internacional para la Normalización (ISO) como modelo de referencia para el establecimiento de una comunicación abierta en diferentes sistemas técnicos.

A finales de los años 70, los fabricantes más destacados en el ámbito de la tecnología de redes tuvieron que hacer frente al problema de que sus dispositivos solo podían conectarse a través de una arquitectura de red privada. Por aquel entonces, ningún fabricante pensó en crear componentes de software y hardware siguiendo las especificaciones de otros fabricantes y un proyecto como Internet presupone, en cambio, ciertos estándares que posibiliten la comunicación.

El modelo de referencia ISO no es propiamente un estándar de red concreto, sino que, en términos abstractos, describe cuáles son los procesos que se han de llevar a cabo para que la comunicación funcione a través de una red y así conseguir un estándar .

Para ello, el modelo de ISO OSI divide el complicado proceso de la comunicación en red en siete estadios denominados capas OSI. En la comunicación entre dos sistemas, cada capa requiere que se lleven a cabo ciertas tareas específicas. Entre ellas se encuentran, por ejemplo, el control de la comunicación, la direccionalidad del sistema de destino o la traducción de paquetes de datos a señales físicas. Sin embargo, el método solo funciona cuando todos los sistemas participantes en la comunicación cumplen las reglas. Estas se establecen en los llamados protocolos, que se aplican a cada una de las capas o que se utilizan en la totalidad de estas.

CAPAS DEL MODELO OSI

Las capas del modelo OSI se leen de forma descendente es decir desde la capa superior hasta la capa inferior, el usuario solo interactúa con la primera y última capa.

CAPA 7 – APLICACIÓN –

Es la capa superior y la que todos los usuarios visualizan, es la interfaz, las aplicaciones que funcionan en la Capa 7 son aquellas con las que los usuarios interactúan directamente, y luego esta capa interactúa con las demás. Un claro ejemplo son los navegadores web como Google Chrome, Firefox y aplicaciones como Skype, Google Teams entre otros.

CAPA 6 – PRESENTACION –

Se encarga de traducir los paquetes recibidos desde la capa 7 a un formato genérico que todas las computadoras leen, para que luego viajen por todas las capas una vez cifrados y comprimidos los datos.

CAPA 5 – SESION –

Maneja la conversación entre un dispositivo y otro remoto creando una sesión en esta capa y comunicándose con la capa de sesión del otro dispositivo, solicitando el acceso que luego es autorizado o no. Esta capa es fundamental para mantener el enlace de los dispositivos que se están transmitiendo archivos.

CAPA 4 – TRANSPORTE –

Se encarga de la coordinación de la transferencia fiable de datos entre los sistemas finales y los hosts. Cuantos datos enviar, a qué velocidad, a dónde va, entre tantos otros. También evalúa el tamaño de los paquetes para que estos tengan el tamaño correcto para las capas inferiores.

CAPA 3 – RED –

En esta capa es donde operan los router y se determina la mejor ruta para enviar los paquetes por la red. Es la capa de direccionamiento lógico, es decir, se incrusta la IP de origen y de destino. Además se encarga de que todos los datos salgan y lleguen correctamente aunque no estén conectados directamente (geográficamente).

CAPA 2 - ENLACE DE DATOS –

Toma la información recopilada en las capas superiores y las transforma en números binarios para ser enviada por la capa física.

Esta capa proporciona la transferencia de datos de nodo a nodo (conectados directamente) y también maneja la corrección de errores de la capa física. Aquí también existen dos subcapas: la capa de Control de acceso al medio (MAC) y la capa de Control de enlace lógico (LLC).

CAPA 1 – FISICA –

Se encuentra en la parte inferior, representa los aspectos eléctricos y físicos del sistema, es la capa de transmisión binaria de los datos por los medios reconocidos (WiFi, cables de red, entre otros). En resumen, se encarga de las conexiones físicas
entre los dispositivos de red como desde el tipo de cable, el enlace de radiofrecuencia, a distribución de pines, voltajes entre otros.

PROTOCOLO TCP/IP

Los protocolos son conjuntos de normas para formatos de mensaje y procedimientos que permiten a las máquinas y los programas de aplicación intercambiar información. Cada máquina implicada en la comunicación debe seguir estas normas para que el sistema principal de recepción pueda interpretar el mensaje.

TCP/IP significa Protocolo de Control de Transmisión/Protocolo de Internet.

¿Qué es el protocolo TCP?

En los inicios de internet toda la comunicación era unidireccional. Es decir, se conocía al emisor de la información, pero no la persona ni el dispositivo que pudiera recibirla**,** hasta el año 1973, cuando los informáticos Robert E. Kahn y Vinton G. Cerf publicaron su primera versión del protocolo TCP en el marco de su trabajo de investigación.

El protocolo TCP o protocolo de control de transmisión es un acuerdo estandarizado de transmisión de datos entre distintos participantes de una red informática.

El estado actual de desarrollo del protocolo TCP permite establecer una conexión entre dos puntos terminales en una red informática común que posibilite un intercambio mutuo de datos. En este proceso, cualquier pérdida de datos se detecta y resuelve, por lo que se considera un protocolo fiable. Dentro de la familia de protocolos de Internet, el TCP, junto con el UDP y el SCTP forma el grupo de los protocolos de transporte, que, según el modelo OSI, se ubican en la capa de transporte dentro de la arquitectura de red. Como el protocolo TCP se combina casi en todos los casos con el protocolo de Internet (IP) y esta conexión forma la base de la gran mayoría de redes locales y servicios de red, es común hablar del conjunto de protocolos TCP/IP**,** aunque en realidad se haga referencia a la familia de protocolos de Internet.

TCP/IP y sus características

El modelo TCP/IP es la familia de protocolos de internet que permite la transmisión de datos entre computadoras este modelo es ideal para la poderosa y descentrada red que es internet.

El protocolo del diseño de TCP/IP se basa en el protocolo de internet IP y en el protocolo de control de transmisión.

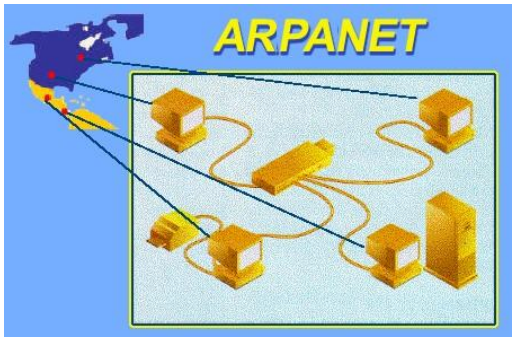
TCP/IP tiene 4 capas esta arquitectura de capas a menudo es comparada con el modelo OSI de 7 capas.

Nº de capa	OSI
7	Aplicación
6	Presentación
5	Sesión
4	Transporte
3	Red
2	Enlace de datos
1	Física

TCP/IP	Nº de capa
Aplicación	4
Transporte	3
Internet	2
Acceso a la red	1

Podemos afirmar que el modelo TCP/IP es la base de internet y sirve para enlazar computadoras que utilizan distintos tipos de Sistemas Operativos tales como:

Se utilizan en minicomputadoras y computadoras centrales y fue insertada en la RED ARPANET la cual fue creada en el departamento de EE.UU como video de comunicación de los diferentes organismos del país .



TCP/IP obtiene 4 capas de abstracción o niveles cada nivel se ve encargado determinados aspectos de la comunicación y a la vez brinda un servicio específico a la capa superior ellas son:

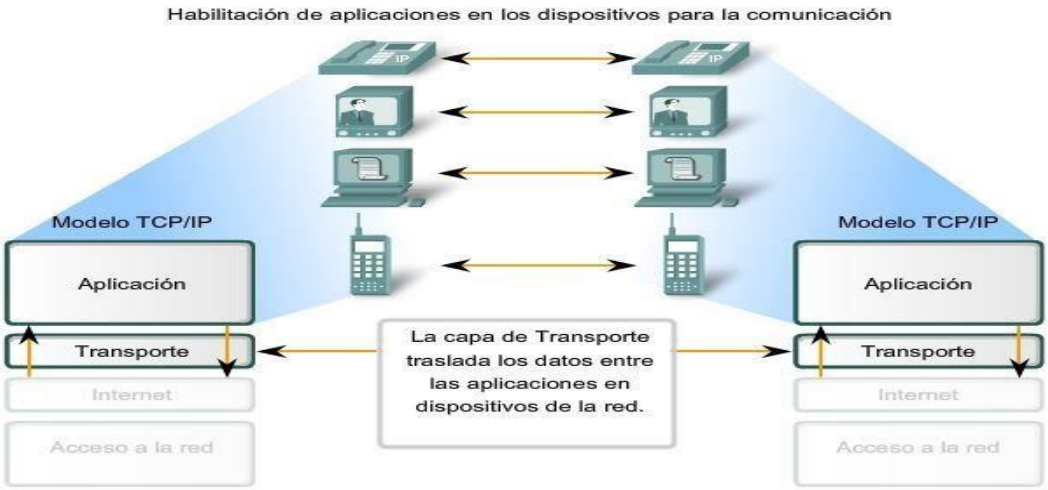
CAPA DE APLICACIÓN:

Maneja protocolos de alto nivel aspectos de representación, codificación, control de dialogo .

El TCP/IP influye no solo en las especificaciones del internet y capa de transporte, sino que también en las especificaciones referida a las APLICACIONES comunes, el TCP obtiene protocolos que soporta la transferencia de archivos, emails, conexiones remotas además de FTP (Protocolo Transferencia de Archivo), TFTP(Protocolo Transferencia de Archivo Trivial), NFS(Sistema de Archivo de Red), es utilizado por sistemas de archivos distribuidos en un entorno de red SMTP(Protocolo Transferencia de correo electrónico), TELNET(emulación determinal) ,DNS(Sistema de Nombre de Dominio) es jerárquico como sistema para computadoras.

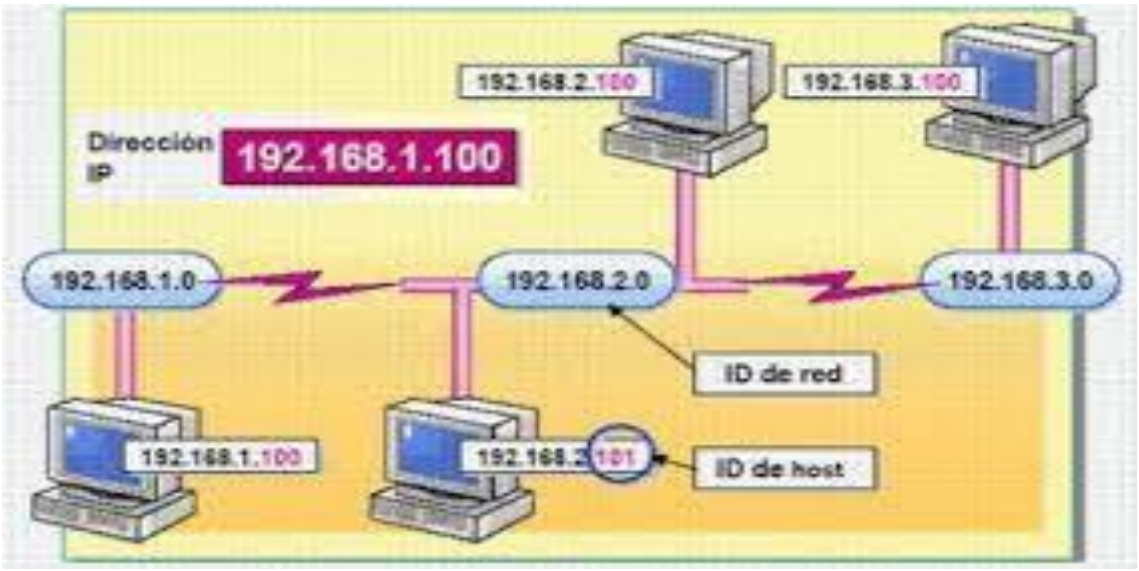
CAPA DE TRANSPORTE:

Son proporcionales de servicio de transporte desde el HOST origen al HOST destino que no siempre están conectados a la misma red



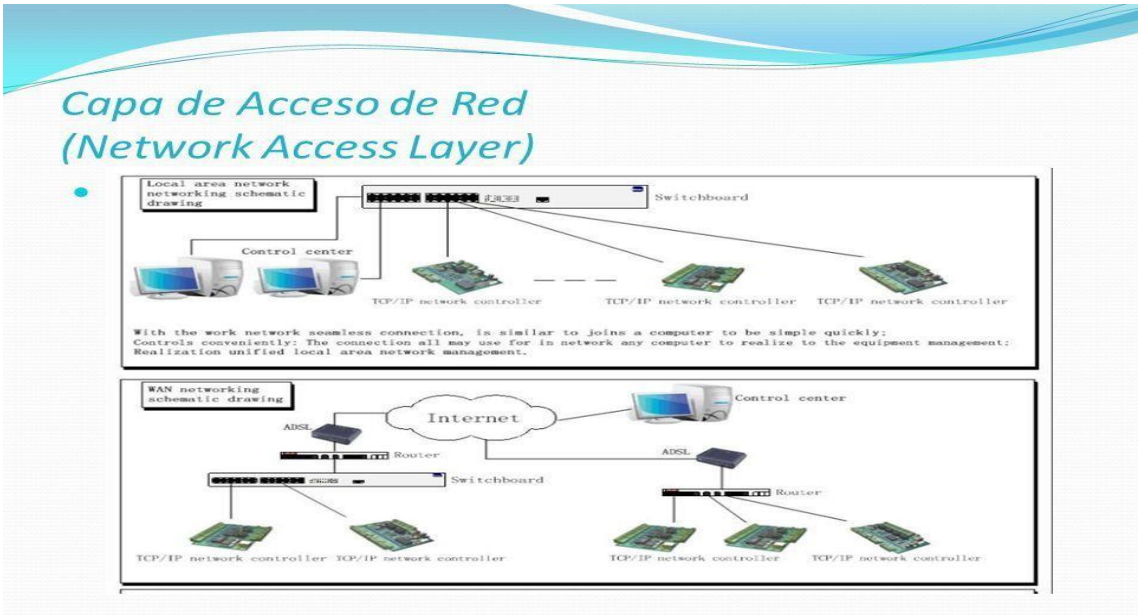
CAPA DE INTERNET:

Se produce la selección de la mejor ruta y la conmutación de paquetes el protocolo especifico que rige esta capa se denomina protocolo de internet ósea IP en esta capa se produce la determinación de la mejor ruta y conmutación de paquetes



CAPA DE ACCESO DE RED:

Es la que se ocupa de todos los aspectos que requiere el paquete IP para realizar un enlace físico el cual influye detalles de la tecnología LAN y WAN.



CARACTERISTICAS DE PROTOCOLO TCP:

- El protocolo TCP está orientado a la conexión y permite una comunicación recíproca entre dos puntos terminales mediante el denominado triple apretón de manos.
- Es fiable, ya que el protocolo garantiza que se transmiten todos los datos de forma íntegra y que el receptor pueda recomponerlos en el orden correcto.
- Permite el monitoreo del flujo de los datos y así evitar la saturación de la red.
- En la mayoría de los casos, el protocolo se suma al protocolo de Internet (IP), por lo que a menudo se habla del conjunto de protocolos TCP/IP.
- Permite que los datos se formen en segmentos de longitud variada para "entregarlos" al protocolo IP.
- Envía los datos en segmentos individuales con un tamaño máximo de 1500 bytes (incluidos los encabezados).
- En el modelo OSI, el TCP se clasifica en la capa de transporte (capa 4).
- Permite multiplexar los datos, es decir, que la información que viene de diferentes fuentes (por ejemplo, aplicaciones) en la misma línea pueda circular simultáneamente.
- Por último, permite comenzar y finalizar la comunicación amablemente.

PROTOCOLO IP:

El protocolo de IP (Internet Protocolo) es la base fundamental de la Internet. Porta datagramas de la fuente al destino. El nivel de transporte parte el flujo de datos en datagramas. Durante su transmisión se puede partir un datagrama en fragmentos que se montan de nuevo en el destino. Las principales características de este protocolo son:

- Protocolo orientado a no conexión.
- Fragmenta paquetes si es necesario.
- Direccionamiento mediante direcciones lógicas IP de 32 bits.
- Si un paquete no es recibido, este permanecerá en la red durante un tiempo finito.
- Realiza el "mejor esfuerzo" para la distribución de paquetes.
- Tamaño máximo del paquete de 65635 bytes.
- Sólo ser realiza verificación por suma al encabezado del paquete, no a los datos éste que contiene.

El Protocolo Internet proporciona un servicio de distribución de paquetes de información orientado a no conexión de manera no fiable. La orientación a no conexión significa que los paquetes de información, que será emitido a la red, son tratados independientemente, pudiendo viajar por diferentes trayectorias para llegar a su destino. El término no fiable significa más que nada que no se garantiza la recepción del paquete.

La unidad de información intercambiada por IP es denominada datagrama. Tomando como analogía los marcos intercambiados por una red física los datagramas contienen un encabezado y una área de datos. IP no especifica el contenido del área de datos, ésta será utilizada arbitrariamente por el protocolo de transporte.

Direcciones IP

Para que en una red dos computadoras puedan comunicarse entre sí ellas deben estar identificadas con precisión Este identificador puede estar definido en niveles bajos (identificador físico) o en niveles altos (identificador lógico) de pendiendo del protocolo utilizado. TCP/IP utiliza un identificador denominado dirección internet o dirección IP, cuya longitud es de 32 bites. La dirección IP identifica tanto a la red a la que pertenece una computadora como a ella misma dentro de dicha red.

Tomando tal cual está definida una dirección IP podría surgir la duda de cómo identificar qué parte de la dirección identifica a la red y qué parte al nodo en dicha red. Lo anterior se resuelve mediante la definición de las "Clases de Direcciones IP". Para clarificar lo anterior veamos que una red con dirección clase A queda precisamente definida con el primer octeto de la dirección, la clase B con los dos primeros y la C con los tres primeros octetos. Los octetos restantes definen los nodos en la red específica.

PROTOCOLO IPV4:

IPv4 es la versión 4 del Protocolo de Internet (**IP** o **I**nternet **P**rotocol) y constituye la primera versión de IP que es implementada de forma extensiva. **IPv4** es el principal protocolo utilizado en el Nivel de Red del Modelo TCP/IP para Internet. Fue descrito inicial mente en el RFC 791 elaborado por la Fuerza de Trabajo en Ingeniería de Internet (**IETF** o **I**nternet **E**ngineering **T**ask **F**orce) en Septiembre de 1981, documento que dejó obsoleto al RFC 760 de Enero de 1980.

IPv4 es un protocolo orientado hacia datos que se utiliza para comunicación entre redes a través de interrupciones (switches) de paquetes (por ejemplo a través de Ethernet). Tiene las siguientes características:

- Es un protocolo de un servicio de datagramas no fiable (también referido como de *mejor esfuerzo*).
- No proporciona garantía en la entrega de datos.
- No proporciona ni garantías sobre la corrección de los datos.
- Puede resultar en paquetes duplicado o en desorden.

Todos los problemas mencionados se resuelven en el nivel superior en el modelo TCP/IP, por ejemplo, a través de **TCP** o **UDP**.

El propósito principal de **IP** es proveer una dirección única a cada sistema para asegurar que una computadora en Internet pueda identificar a otra.

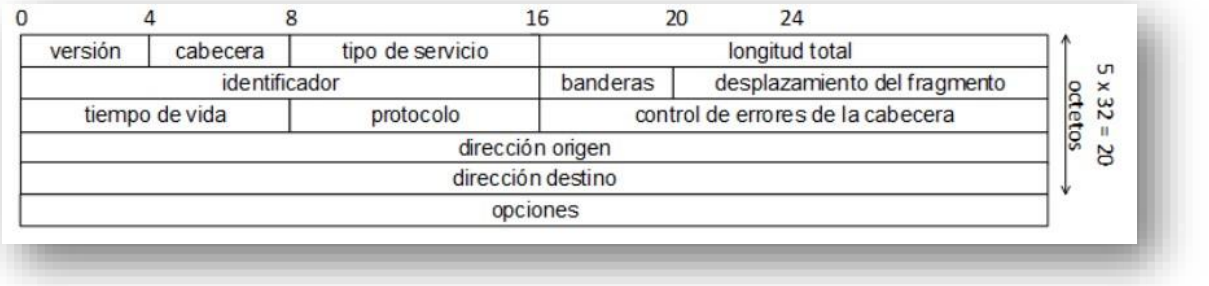


FIGURA 1: CABECERA DE IPV4. 1

PROTOCOLO IPV6:

Como se ha comentado, IPv6 fue diseñado como una evolución natural a IPv4. Es decir, todo lo que funcionaba perfectamente en IPv4 se ha mantenido, lo que no funcionaba se ha eliminado, y se ha tratado de añadir nuevas funciones manteniendo la compatibilidad entre ambos protocolos.

Las características principales de IPv6 son:

- Mayor espacio de direcciones.
- Optimización del direccionamiento *multicast* y aparición del direccionamiento *anycast*.
- Autoconfiguración de los nodos.
- Seguridad intrínseca en el núcleo del protocolo
- Calidad de servicio y clases de servicios.
- Paquetes eficientes y extensibles.
- Encaminamiento más eficiente en la red troncal.
- Remuneración y *multihoming*, que facilita el cambio de proveedor de servicios.
- Características de movilidad.

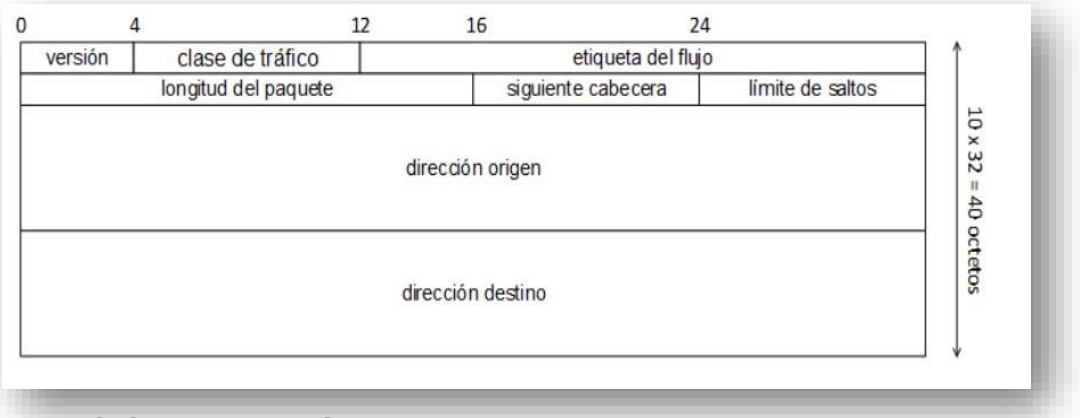
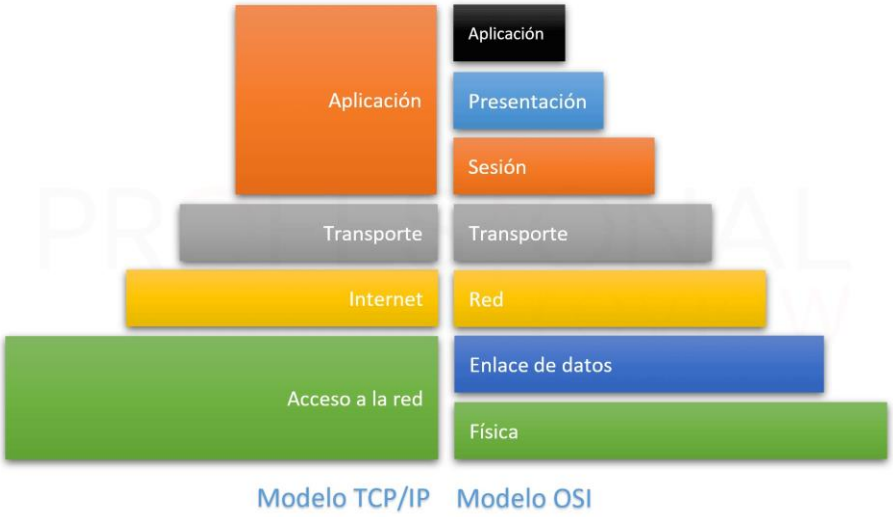


FIGURA 2: CABECERA DE IPV6. 1

Funcionamiento de TCP/IP

El TCP/IP define las reglas para el intercambio de datos entre ordenadores que a su vez permiten el acceso a Internet cada vez que se necesita enviar un mensaje o recibir información de otro ordenador host, independientemente de la arquitectura del sistema operativo instalado; proporcionando una comunicación confiable compilando datos en paquetes y transportándolos al destino correcto.



La capa de **Acceso a la Red** es la primera capa del modelo y ofrece la posibilidad de acceso físico a la red, especificando el modo en que los datos deben enrutarse independientemente del tipo de red utilizado.

- Controla todos los aspectos relacionados al enlace físico con los medios de red. • Define la interfaz con el hardware de la red para acceder al medio de transmisión.
- Reúne las capas de Enlace de Datos y Física del modelo OSI.

La capa de **Red o Internet** proporciona el paquete de datos o datagramas y administra las direcciones IP. (Los datagramas son paquetes de datos que constituyen el mínimo de información en una red). Engloba protocolos como IP, ARP, ICMP, IGMP y RARP.

- Proporciona direccionamiento jerárquico.
- Halla la ruta más confiable entre origen y destino.

La siguiente capa **Transporte** permite conocer el estado de la transmisión así como los datos de enrutamiento y utilizan los puertos para asociar un tipo de aplicación con un tipo de dato.

- Proporciona servicios de control de flujo y de transporte entre origen y destino, creando un circuito virtual.
- Segmenta y reensambla los datos.

La capa superior de la pila TCP/IP es la capa de **Aplicación**, que permite a los usuarios intercambiar datos entre aplicaciones involucradas en el sistema de comunicación.

- Se desarrollan procesos de alto nivel referidos a la presentación, codificación y control de dialogo.
- Suministra las aplicaciones de red TIP Telnet, FTP o SMTP, que se comunican con las capas anteriores (protocolos TCP o UDP).

OTROS PROTOCOLOS

UDP

El protocolo de datagramas de usuario, abreviado como UDP, es un protocolo que permite la transmisión sin conexión de datagramas en redes basadas en IP. Para obtener los servicios deseados en los hosts de destino, se basa en los puertos que están listados como uno de los campos principales en la cabecera UDP. Como muchos otros protocolos de red, UDP pertenece a la familia de protocolos de Internet, por lo que debe clasificarse en el nivel de transporte y, en consecuencia, se encuentra en una capa intermedia entre la capa de red y la capa de aplicación.

El protocolo UDP se utiliza para transmitir datagramas de forma rápida en redes IP y funciona como una alternativa sencilla y sin retardos del protocolo TCP. Se usa principalmente para consultas DNS, conexiones VPN y para el streaming de audio y vídeo.

HTTP

El protocolo HTTP nos permite realizar una petición de datos y recursos, como pueden ser documentos HTML. Es la base de cualquier intercambio de datos en la Web, y un protocolo de estructura clienteservidor, esto quiere decir que una petición de datos es iniciada por el elemento que recibirá los datos (el cliente), normalmente un navegador Web.

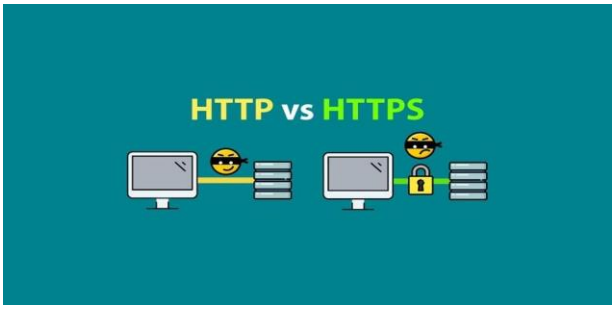
Clientes y servidores se comunican intercambiando mensajes. Los mensajes que envía el cliente,
normalmente un navegador Web, se llaman peticiones, y los mensajes enviados por el servidor se llaman respuestas.

Cada petición individual se envía a un servidor, el cual la gestiona y responde. Entre cada petición y respuesta, hay varios intermediarios, normalmente denominados proxies, los cuales realizan distintas funciones, como: gateways o caches.

DIFERENCIAS ENTRE HTTP Y HTTPS

La principal diferencia entre HTTP y HTTPS es la seguridad. El protocolo HTTPS impide que otros usuarios puedan interceptar la información que se transfiere entre el cliente y el servidor web. Además de mostrarse HTTPS en la barra de direcciones, también hay un elemento que diferencia claramente una web segura y otra que no lo es: un candado verde.

Para que una web funcione bajo el protocolo HTTPS es necesario tener instalado un Certificado SSL. Este certificado de seguridad es el encargado de cifrar o encriptar las conexiones entre el navegador y servidor web impidiendo que nadie pueda interceptar la información que se transfiere entre ambos. De este modo, todos los datos personales, bancarios o cualquier otro tipo de información sensible que se intercambie estará protegida.



CRITERIOS DE DISEÑO DE REDES

Relación entre el Modelo OSI y los elementos de una Red

Las capas del modelo OSI, contienen una estrecha relación con los elementos que podemos encontrar en una red. Estos se encargan de llevar a cabo algunas de las funciones de sus respectivas capas.

Capa Física- Hubs y Repetidores

En la capa física, se definen las especificaciones eléctricas, mecánicas, de procedimiento y funcionales para activar, mantener y desactivar el enlace físico entre sistemas finales de una red, y se trabaja la topología de la misma. Por lo tanto, los repetidores y los hubs (concentradores) pertenecen a esta, ya que se encargan, de cierta forma, de ampliar la "longitud" de la red. Ya sea conectando dos segmentos de una misma red (repetidores), o centralizando el cableado de una red y ampliándolo (concentradores).

Capa de Enlace de Datos- Switch y Bridge

En la capa de Enlace de Datos se trabaja el direccionamiento físico de una red. Aquí podemos encontrar los Switch (enlazadores) y los Bridge (puentes). Estos, como los repetidores y los concentradores, permiten conectar dos segmentos de red, pero a diferencia de ellos, seleccionan el tráfico que pasa de un segmento a otro, haciendo el trabajo de direccionamiento y reduciendo considerablemente el tráfico en los segmentos de red conectados al dispositivo.

Capa de Red- Routers

En la capa de Red se proporciona conectividad y selección de ruta entre dos sistemas de hosts que pueden estar ubicados en redes geográficamente distintas. Aquí operan los router (encaminadores) que se encargan de asegurar el enrutamiento de paquetes entre redes o determinar la ruta que debe tomar el paquete de datos.

Capa de Aplicación- Gateway

Estas pasarelas, cumplen la misma función que los encaminadores, pero además traducen la información del protocolo utilizado en la red inicial, al protocolo usado en la red de destino. Una pasarela (Gateway) modifica el empaquetamiento de la información de la red de origen para

acomodarse a la sintaxis de la red de destino, por lo que suelen trabajar en el nivel más alto del modelo OSI (el de Aplicación). De esta forma, pueden conectar redes con arquitecturas completamente distintas.

ACCESS POINT

El **Access Point** es un dispositivo para redes inalámbricas, un dispositivo que interconecta terminales inalámbricos a una red. Proveen conectividad dentro de las organizaciones para dispositivos inalámbricos de todo tipo. Estos se usan para conectar a servicios de banda ancha como IP sobre cable, ADSL. Un **Access Point** usado en una casa puede dar la posibilidad de conectar a una empresa a través de una red privada virtual.

La arquitectura física

En un **Access Point** se pueden identificar cuatro componentes:

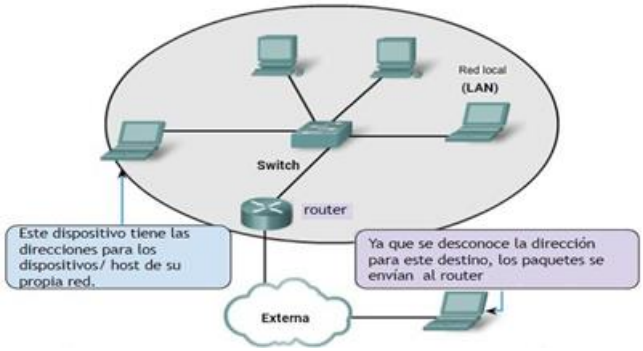
- **Puertos de entrada:** Lleva a cabo las funciones de la capa física resistente en la terminación de un enlace físico de entrada a un router, también realiza la función de búsqueda y reenvío así ya se por un paquete reenviado dentro del entramado de conmutación.
- **Puertos de salida:** Es el que almacena los paquetes que le reenviaron por medio del puerto de conmutación y los transfiere al enlace de salida.

ROUTERS (encaminadores)

¿Qué son y para qué sirven?

Router (encaminador) 1

Los Routers es un equipo informático configurado para permitir que las máquinas de una **red local (LAN)** conectadas a él tengan un acceso hacia una **red exterior**, generalmente realizando para ello operaciones de traducción de direcciones **IP**.



Router

Sus principales características son:

- Se trata de una computadora que interconecta redes radicalmente distintas.
- Trabajan en el modelo más alto del modelo OSI (el de aplicación).
- Cuando se habla de Default Gateway a nivel de redes de área local, en realidad se está hablando de **routers**.

REPETIDORES

Forman parte del grupo de dispositivos de interconexión que permiten conectar segmentos de una misma red, o redes diferentes.

Según las telecomunicaciones, los repetidores se pueden definir de las siguientes maneras:

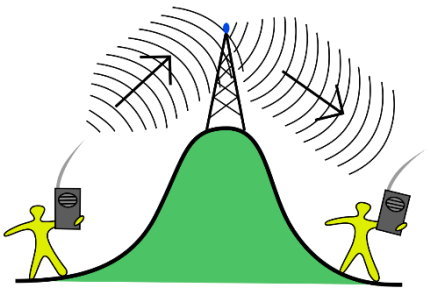
1. Un dispositivo analógico que amplifica una señal de entrada sea analógica o digital.
2. Un dispositivo digital que amplifica conforma, re-temporiza o lleva a cabo una combinación entre las funciones anteriores sobre una señal digital de entrada para su retransmisión.

¿Por qué surge el repetidor?

El repetidor surge por la dificultad de transmitir una señal desde un emisor hasta un receptor que se encuentre a una gran distancia o que para llegar él sea necesario pasar por obstáculos geográficos.

¿Cuál es su función?

La función que cumple es regenerar (repetir) la señal transmitida evitando su atenuación, así se puede ampliar la longitud del cable que soporta la red. Por ejemplo, entre dos dispositivos hay un cable de 150 metros, para que no exista mucha atenuación o interferencia en la señal entre los aparatos, se necesita un repetidor instalado en el centro del cable que lo divida en dos partes que no excedan el límite de la longitud del segmento que en este caso sería 100mb.



Repetidores 1

Cuando la señal recibida es digital, al repetidor se le llama regenerador, ya que la señal de salida es una señal regenerada a partir de la de entrada. Para eso, el repetidor convierte la señal óptica en eléctrica y la regenera en señal óptica para retransmitirla.

Características Principales

- Los repetidores trabajan a nivel 1 del modelo OSI.
- Aíslan entre los segmentos los problemas eléctricos que pudiera haber en alguno de ellos.
- El repetidor cuenta con dos entradas que conectan con segmentos ethernet por medio de cables drop y transceivers. Se puede instalar diferentes transceivers para interconectar dos segmentos de medios físicos.
- El repetidor tiene como mínimo una salida ethernet para el cable amarillo y otra para el teléfono.
- Con un repetidor modular se puede centralizar y estructurar todo el cableado de un edificio.

Repetidor con dos entradas 1

Tipos de repetidores.

Repetidores wifi, repetidores del fondo marino para los cables transcontinentales e instalaciones (edificios, torres, equipos eléctricos y electrónicos, antenas, etc) que repiten señales de televisión, radio y telefonía móvil.

Señales con las que trabaja.

Señal eléctrica, radioeléctrica y luminosa-óptica (digital)

BRIDGES (puentes)

Es un dispositivo de interconexión de redes que opera en la capa 2 del modelo OSI. Un bridge conecta dos o más redes entre sí formando una sola subred (permite conexión entre equipos sin necesidad de routers).

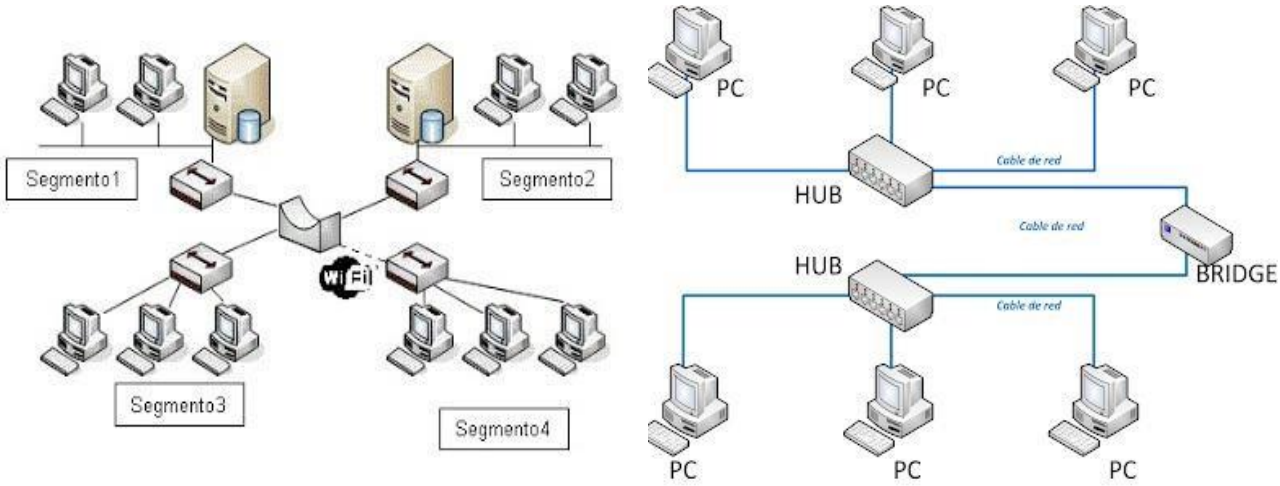
¿Cuáles son sus funciones?

- Divide la red LAN en segmentos o subredes. Cuando una LAN se hace demasiado grande, en cuanto a número de puestos o extensión, debe ser dividida para optimizar su funcionamiento.
- Interconecta dos redes LAN, pudiendo tener protocolos de nivel dos o medios de transmisión distintos.
- Controla las tramas defectuosas, verificando los datos para determinar si les corresponde o no cruzar el puente.

Las ventajas que introducen los puentes en redes locales grandes, derivan de la división en segmentos de red distintos de la red global. De esta forma, la lógica electrónica del puente reduce el traficó general, ya que los segmentos no involucrados en una transmisión concreta se mantienen libres de tráfico.

Básicamente los puentes reciben todos los paquetes de información enviados por cada red acoplada a él, y los reenvían selectivamente entre las LAN que incluyan el equipo terminal al cual va dirigida la transmisión, descartando o filtrando aquellos que no necesitan ser retransmitidos o haya detectado que son defectuosos. Por ejemplo, cuando un puente recibe información que va dirigida al mismo segmento de red del que procede, éste comprueba que el emisor y el receptor del mensaje se encuentran en una misma rama y descarta el mensaje. Si el destinatario del mensaje se encontrara en un segmento distinto, el puente al verificar esta situación, la transmitiría por el puerto adecuado.

Cuando un puente inicia su función por primera vez, no tiene ninguna información sobre los equipos de las redes que interconecta. Sin embargo, a medida que va analizando tramas y comprobando las direcciones de procedencia, crea una base de datos o mapa de direcciones que usará posteriormente. Si en alguna ocasión desconoce la dirección a la que debe enviar una trama, transmitirá por todos sus puertos, de esta forma garantiza que lleguen los datos a su destino. Cuando el host de destino envía una señal de confirmación de recepción, podrá incorporar su dirección a su memoria.



El uso de bridge se justifica cuando:

- Se quieren unir dos redes sin un router.
- Cuando se desea aislar el tráfico de red que conecta el puente

Cuando un puente debe traspasar una trama de un segmento a otro de la red ejecuta las acciones siguientes:

- Almacena la trama recibida por cualquier puerto para su posterior análisis.
- Comprueba la integridad de la trama. Si está incorrecta o incompleta la elimina.
- Reconfigura el formato de la trama al segmento de red destino.
- Reexpide la trama al segmento de red accesible por alguno de sus puertos.

Se le suele denominar “Separación de los dominios de colisión” al aislamiento efectuado por los bridges o dispositivos de red de nivel superior, debido a que dos host colocados en segmentos de red diferentes no pueden colisionar en su acceso a la red puesto que las tramas no pueden atravesar segmentos mientras que el puente que los está uniendo no tome la decisión de conmutarlos

Tipos de Bridge

Por su configuración

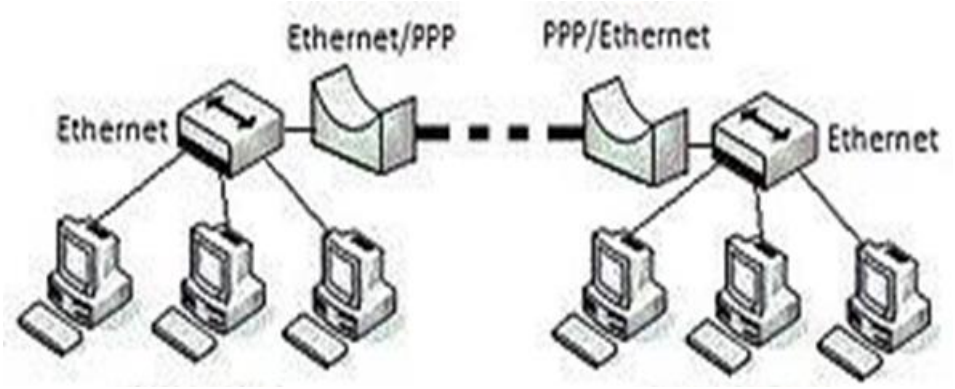
Un bridge o puente, según su **configuración** puede ser:

- **Transparente**: No requiere ninguna configuración para su funcionamiento
- **No transparente**: Necesita que la trama lleve información sobre el modo que ha de ser reenviada.

Por su ámbito

Según el **ámbito** pueden ser:

- **Locales**: Une dos o más segmentos de una misma red
- **Remotos**: Se divide en dos partes, cada una de ellas tiene conectado un segmento de red, y se unen a través de la línea de una red WAN



Ejemplo de configuración remota- Bridge 1

Ventajas y desventajas de las redes conectadas con Bridges

Ventajas

- En general, es un dispositivo de bajo precio.
- Aísla dominios de colisión al segmentar la red.
- No necesita configuración previa.
- Control de acceso y capacidad de gestión de la red.

Desventajas

- No se limita el número de reenvíos mediante broadcast.
- Difícilmente escalable para redes muy grandes.
- El procesado y almacenamiento de datos introduce retardos.
- Las redes complejas pueden suponer un problema. La existencia de múltiples caminos entre varias LAN puede hacer que se formen bucles.

HUBS (Concentradores)

Un HUB, o más conocido en español como concentrador, es un dispositivo de emisión bastante sencillo mediante el cual podremos conectar varios aparatos entre sí, para que puedan comunicarse. Es capaz de crear una red de ordenadores conectados y con posibilidad de ampliarse mediante otros dispositivos similares. Es decir, permite **centralizar el cableado de una red y poder ampliarla**.

Si recordamos qué es el **modelo OSI** y en qué consiste, el HUB trabaja en la capa física de este modelo, o en la capa de acceso al medio si hablamos del **modelo TCP/IP**.

Función

Un concentrador se encarga de recibir una señal de datos y repetirla para enviarla por sus diferentes puertos. Entonces, básicamente estamos hablando de un **repetidor**. Funciona como un punto central de conexión y repite la señal que recibe a tantos puertos como equipos haya conectados en ellos. Luego cada equipo se encargará de identificar si la información que recibe es útil y le pertenece, o va destinada a otro. Dado que cada paquete está siendo enviado a través de cualquier otro puerto, aparecen **las colisiones de paquetes** como resultado, que impiden en gran medida la fluidez del tráfico. Cuando dos dispositivos intentan comunicar simultáneamente, ocurrirá una colisión entre los paquetes transmitidos, que los dispositivos transmisores detectan. Al detectar esta colisión, los dispositivos dejan de transmitir y hacen una pausa antes de volver a enviar los paquetes.

Tipos de HUBS

Los hubs vienen en tres tipos básicos:

- **Pasivo:** Sirve sólo como punto de conexión física. No manipula o visualiza el tráfico que lo cruza. No amplifica o limpia la señal. Se utiliza sólo para compartir los medios físicos. En sí, un hub pasivo no requiere energía eléctrica.
- **Activo:** Se debe conectar a un tomacorriente porque necesita alimentación para amplificar la señal entrante antes de pasarla a los otros puertos.
- **Inteligente:** A veces se los denomina "smart hubs". Estos dispositivos básicamente funcionan como hubs activos, pero también incluyen un chip microprocesador y capacidades diagnósticas.

Diferencias entre HUB y SWITCH

Un **HUB** no es capaz de distinguir dónde va dirigida la información. *Este dispositivo se limita a recibir la información y repetirla para todos sus puertos, independientemente de lo que haya conectado en ellos.* A esto se le llamada broadcast, recibir una y enviar a todos. Un problema que tienen los HUB es la rápida saturación del ancho de banda, debido a la repetición masiva de los datos.

Por su parte, un switch es la versión inteligente de un HUB, físicamente es similar, pero en su interior existe un programa informático o firmware que es capaz de entender la información que por él viaja y enviarla solamente al nodo que la necesita. Entonces la ventaja es obvia, el ancho de banda estará mucho más optimizado y seremos capaces de comunicar ordenadores entre sí de forma independiente y sin necesidad de enviar toda la información a todos los puertos.

Por supuesto, un HUB no se puede gestionar, ya que no tiene ningún tipo de software accesible, mientras que un switch sí que tiene esta posibilidad (no todos), éstos apartados incorporan cortafuegos, QoS, MU-MIMO, etc. Es por esto que son los dispositivos más utilizados a día de hoy para crear redes internas cableadas de alta velocidad y eficiencia.

SWITCH (Conmutador)

Capa 2 (modelo OSI – Enlace de datos).

Switch- Capa 2 Modelo OSI 1

Un switch o conmutador es un dispositivo de interconexión, utilizado para conectar equipos en una misma red, formando lo que se conoce como una red de área local (LAN) y cuyas especificaciones técnicas siguen el estándar conocido como Ethernet (o técnicamente IEEE 802.3).

Los puertos son los elementos del switch que permiten la conexión de otros dispositivos al mismo. Como por ejemplo un PC, portátil, un router, otro switch, una impresora y en general cualquier dispositivo que incluya una interfaz de red Ethernet. *A través del switch la información enviada por un host de origen va directamente al host de destino sin replicarse en el resto de los equipos que estén conectados.*

Por lo tanto, la red ya no queda "limitada", y mientras le enviamos datos a un dispositivo, el resto de los equipos de la red pueden enviarse también datos entre sí. Esto se debe a que el switch cuenta con una tabla Mac, en donde se guardan las direcciones físicas de cada dispositivo y de esta forma pueden identificarse.

Para que pueda guardarse estas direcciones, primero tiene que ocurrir una comunicación entre los dispositivos.

Pasos que realiza un Switch

Paso 1: El switch reenvía tramas basándose en la dirección MAC de destino.

A- Si la MAC de destino es un broadcast, multicast o unicast con el destino desconocido (no existe en la tabla de MAC), el switch inundara la red reenviando la trama a todos los puertos, excepto por el que se recibió.
B- Si la dirección MAC de destino es una dirección conocida (existe en la tabla de MAC). A- Si la interfaz de salida en la tabla de direcciones MAC es diferente a la interfaz desde donde la recibió, el switch reenvía la trama a la interfaz de salida.
B-Si la interfaz de salida en la tabla de direcciones MAC es la misma que la interfaz desde donde la recibió, el switch filtra la trama, esto quiere decir que el switch simplemente ignora la trama y no la reenvía.

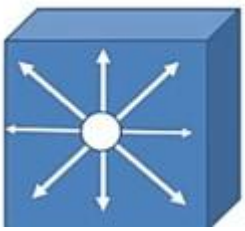
Paso 2: El switch utiliza la siguiente lógica para aprender las entradas de la tabla de direcciones MAC:

A-Reenvía cada trama recibida, examina la dirección MAC de origen y anota la interfaz por donde la trama fue recibida.

B-Si no existe la dirección MAC de origen la tabla agrega la dirección y la interfaz por donde la aprendió.

Paso 3: El switch utiliza STP para prevenir loops (bucles) bloqueando algunas interfaces, es decir, esas interfaces no podrán enviar o recibir tramas.

Capa 3 (modelo OSI- Red)



Switch- Capa 3 Modelo OSI 1

Un switch de Capa 3 hace las funciones de un switch de Capa 2. Además, puede ejecutar enrutamiento estático y enrutamiento dinámico. En otras palabras, un switch de Capa 3 dispone de una tabla de direcciones MAC y de una tabla de enrutamiento IP. Adicional a esto, también controla la comunicación intra-VLAN y el enrutamiento de paquetes entre diferentes VLANs. Un switch que sólo añade enrutamiento estático se conoce como Layer 2+ o Layer 3 Lite. Los switches de Capa 3 incluyen paquetes de enrutamiento y algunas funciones que requieren la

capacidad de comprender la información de la dirección IP de los datos que ingresan al switch; por ejemplo, identificar el etiquetado del tráfico de la VLAN según la dirección IP en vez de configurar un puerto manualmente. Los switches de Capa 3 incrementan la potencia y la seguridad en la medida en que se requiera.

Diferencias entre Switch 3 y router

• Hardware — La diferencia clave entre el Switch capa 3 y el router reside en el hardware. El hardware de un Switch capa 3 combina la lógica de los switches y routers tradicionales, mejorando en parte la lógica de software de un router mediante un hardware de circuito integrado que ofrece un mejor rendimiento en las LANs. Por otra parte, un Switch capa 3, diseñado específicamente para su uso en intranets, normalmente no dispone de puertos WAN y cuenta con un router tradicional. Así que el Switch capa 3 suele ser el más utilizado para soportar enrutamiento entre VLANs.
• Interfaces — Otra de las diferencias entre un Switch capa 3 y un router es que un Switch capa 3 es limitado con respecto a las interfaces que soporta (normalmente sólo Ethernet para RJ45 y fibra monomodo/multimodo), mientras que un router tiene más funciones tales como SDH, SONET, E1/T1 etc. Además, los routers solían ser dispositivos que conectaban la LAN a la WAN y los switches eran sólo dispositivos LAN. • Funcionamiento — El Switch capa 3 examina la dirección MAC del host de destino y envía la trama únicamente a ese destinatario. Un router se remite a la dirección IP de destino en lugar de a su propia dirección MAC, con lo cual generalmente se proporciona más funcionalidad que el simple enrutamiento de paquetes, como por ejemplo la asignación de direcciones IP (DHCP) y el filtrado de cortafuegos.

La principal característica es que **un router trabaja con direcciones IP mientras que en un *switch* ya hemos visto que hace uso de direcciones MAC**. Mientras que las direcciones IP se usan cómo si de un número de teléfono se tratase, las MAC son usadas dentro de la red local.

Por lo tanto, el router es el dispositivo que se encarga de reenviar los paquetes entre distintas redes. **Pueden trabajar junto con HUB y *switches*** y podríamos decir que son el primo más listo, pues además suelen poseer recursos extras, como firewall o WPS.

Los routers son más avanzados pues **combinan en un sólo aparato las funciones de los HUB y los *switches***. Y es que mientras estos últimos se encargan de transmitir frames, el router lo que hace es enviar paquetes a otras redes hasta que llegue a su destino final. Así hay routers que cuentan con un puerto serial al que es posible conectar un modem clásico (si se cae la red principal) o un puerto WAN que permite conectar un cable ADSL.

Relación entre el Modelo OSI y los elementos de una Red

Capa 1 Física- Hubs y Repetidores

Capa 2 de Enlace de Datos- Switch y Bridge

Capa 3 de Red- Routers Capa 7 de Aplicación- Gateway

Las redes por topología y por el grado de autentificación

Topología de red

Las **redes de computadoras** surgieron como una necesidad de interconectar los diferentes hosts de una empresa o institución para poder así compartir recursos y equipos específicos pero los diferentes componentes que van a formar una red se pueden interconectar o unir de diferentes formas, **siendo la forma elegida un factor fundamental que va a determinar el rendimiento y la funcionalidad de la red**. La disposición de los diferentes componentes de una red se conoce con el nombre de **topología de la red**.

La topología idónea para una red concreta va a depender de diferentes factores, como el número de máquinas a interconectar, el tipo de acceso al medio físico que deseemos es por eso que, el concepto de **topología de red** es importante dentro del diseño de redes de computadoras (interconexión de nodos). Es por esta razón que es **fundamental conocer los diferentes tipos de topologías de red** ya que estas definen la manera en que las computadoras se encuentran **conectadas entre sí y de qué manera intercambian los datos**.

Estas funcionan como una familia de comunicación, que define cómo se va a diseñar la red tanto de manera física, como de manera lógica.

En pocas palabras, es la manera en que vamos a tender el cableado que conectará a las computadoras que forman parte de una red a los dispositivos encargados de distribuir está información, como lo son el hub, el switch o el router.

Tipos de topología de red

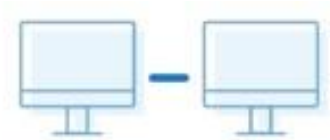
Según sea la distribución que tengamos pensada para el **diseño de una red**, será utilizado un tipo de **topología** específica.

Entre ellas se encuentran dos categorías, **físicas y lógicas**.

Físicas

Punto a punto

Las redes **punto a punto** son aquellas que responden a un tipo de arquitectura de red en las que cada canal de datos se usa para comunicar **únicamente dos nodos** (uno a uno), en clara oposición a redes multipunto, en las cuales cada canal de datos se puede usar para comunicarse con diversos nodos.



En una red punto a punto, los dispositivos en red actúan como socios iguales, o pares entre sí. Como pares, cada dispositivo puede tomar el rol de emisor o la función de receptor, es decir, un dispositivo puede tanto enviar como recibir los datos y viceversa.

- Las redes punto a punto son relativamente fáciles de instalar y operar. A medida que las redes crecen, las relaciones punto a punto se vuelven más difíciles de coordinar y operar. Su eficiencia decrece rápidamente a medida que la cantidad de dispositivos en la red aumenta.
- Los enlaces que interconectan los nodos de una red punto a punto se pueden clasificar en tres tipos según el sentido de las comunicaciones que transportan: o ***Simplex***: la transacción sólo se efectúa en un solo sentido.
  o ***Half-duplex***: la transacción se realiza en ambos sentidos, pero de forma alternativa, es decir solo uno puede transmitir en un momento dado, no pudiendo transmitir los dos al mismo tiempo. o ***Full-duplex***: la transacción se puede llevar a cabo en ambos sentidos simultáneamente.

CARACTERÍSTICAS DE LA RED PUNTO A PUNTO

- Se utiliza en redes de largo alcance (WAN).
- Los algoritmos de encaminamiento suelen ser complejos, y el control de errores se realiza en los nodos intermedios además de los extremos.
- Las estaciones reciben sólo los mensajes que les entregan los nodos de la red.
  Estos previamente identifican a la estación receptora a partir de la dirección de destino del mensaje.
- La conexión entre los nodos se puede realizar con uno o varios sistemas de transmisión de diferente velocidad, trabajando en paralelo.
- Los retardos se deben al tránsito de los mensajes a través de los nodos intermedios.
- La conexión extremo a extremo se realiza a través de los nodos intermedios, por lo que depende de su fiabilidad.
- Los costos del cableado dependen del número de enlaces entre las estaciones. Cada nodo tiene por lo menos dos interfaces.

VENTAJAS DE LA RED PUNTO A PUNTO

- Fáciles de configurar.
- Menor complejidad.

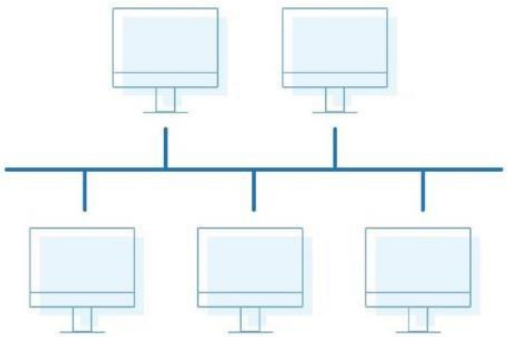
- Menor costo dado que no se necesita dispositivos de red ni servidores dedicados.

DESVENTAJAS DE LA RED PUNTO A PUNTO

- Administración no centralizada.
- No son muy seguras.
- Todos los dispositivos pueden actuar como cliente y como servidor, lo que puede ralentizar su funcionamiento.
- No son escalables
- Reducen su rendimiento

Bus (O lineal)

Una red **en bus** es aquella topología que se caracteriza por tener un **único canal de comunicaciones** (denominado bus, troncal o backbone) al cual se conectan los diferentes dispositivos. De esta forma todos los dispositivos comparten el **mismo canal para comunicarse entre sí**.



VENTAJAS DE LA RED EN BUS

- Facilidad de implementación y crecimiento.
- Simplicidad en la arquitectura.
- Es una red que no ocupa mucho espacio.

DESVENTAJAS DE LA RED EN BUS

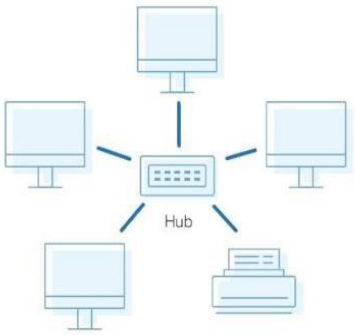
- Hay un límite de equipos dependiendo de la calidad de la señal.
- Puede producirse degradación de la señal.
- Complejidad de reconfiguración y aislamiento de fallos.
- Limitación de las longitudes físicas del canal.
- Un problema en el canal usualmente degrada toda la red.
- El desempeño se disminuye a medida que la red crece.
- El canal requiere ser correctamente cerrado (caminos cerrados).
- Altas pérdidas en la transmisión debido a colisiones entre mensajes.

Estrella

Una red **en estrella** es una red de computadoras donde las estaciones están conectadas **directamente a un punto central** y todas las comunicaciones se hacen necesariamente **a través de ese punto** (conmutador, repetidor o concentrador).

Los dispositivos **no están directamente conectados entre sí**, además de que no se permite tanto tráfico de información. Dada su transmisión, una red en estrella activa tiene un nodo central "activo" que normalmente tiene los medios para prevenir problemas relacionados con el eco.

Se utiliza sobre todo para redes locales (LAN). La mayoría de las redes de área local que tienen un conmutador (*switch*) o un concentrador (*hub*) siguen esta topología. El punto o nodo central en estas sería el switch o el hub, por el que **pasan todos los paquetes de usuarios**.



VENTAJAS DE RED EN ESTRELLA

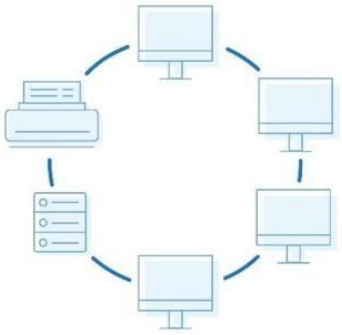
- Posee un sistema que permite agregar nuevos equipos fácilmente.
- Reconfiguración rápida.
- Fácil de prevenir daños y/o conflictos, ya que no afecta a los demás equipos si ocurre algún fallo.
- Centralización de la red.
- Fácil de encontrar fallos.

DESVENTAJAS DE RED EN ESTRELLA

- Si el hub (repetidor) o switch central falla, toda la red deja de transmitir.
- Es costosa, ya que requiere más cables que las topologías en bus o anillo.
- El cable viaja por separado del concentrador a cada computadora.

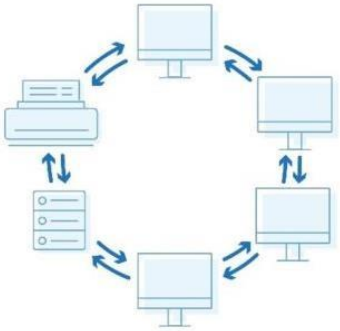
Anillo (O circular)

Una red **en anillo** es una topología de anillo en la que cada estación tiene una **única conexión de entrada y otra de salida** en anillo. Cada estación tiene un receptor y un transmisor que hace la función de traductor, pasando la señal a la siguiente estación.



En este tipo de red la comunicación se da por **el paso de un *token* o testigo**, que se puede conceptualizar como un cartero que pasa recogiendo y entregando paquetes de información, de esta manera se evitan eventuales pérdidas de información debidas a colisiones.

En un **anillo doble** (*Token ring*), dos anillos permiten que los datos se envíen en ambas direcciones (*Token passing*). Esta configuración crea **redundancia** (tolerancia a fallos).



VENTAJAS DE RED EN ANILLO

- El sistema provee un acceso equitativo para todas las computadoras.
- El rendimiento no decae cuando muchos usuarios utilizan la red.
- Arquitectura muy sólida.
- Facilidad para la fluidez de datos.
- Sistema operativo caracterizado con un único canal.

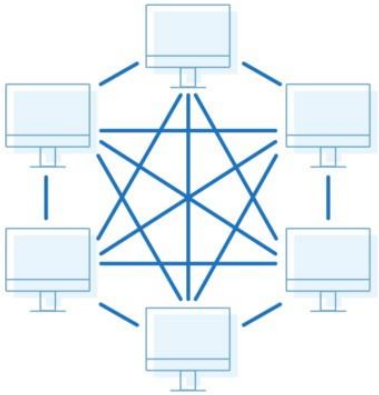
DESVENTAJAS DE RED EN ANILLO

- Longitudes de canales (si una estación desea enviar a otra, los datos tendrán que pasar por todas las estaciones intermedias antes de alcanzar la estación de destino).
- El canal usualmente se degradará a medida que la red crece.
- Difícil de diagnosticar y reparar los problemas.
- Si se encuentra enviando un archivo podrá ser visto por las estaciones intermedias antes de alcanzar la estación de destino.
- La transmisión de datos es más lenta que en las otras topologías (Estrella, Malla, Bus, etc), ya que la información debe pasar por todas las estaciones intermedias antes de llegar al destino.

Malla

Una red **en malla** es una topología de red en la que **cada nodo** está conectado a **todas los nodos**, cada servidor tiene sus **propias conexiones** con todos los demás servidores, gracias a esto ante cualquier fallo en un nodo, la red puede seguir funcionando, por lo tanto, **no cuenta con un nodo central**, esto hace que sea una red muy confiable.

Internet usa esta topología para interconectar las diferentes compañías telefónicas y proveedoras de Internet, mediante enlaces de fibra óptica.



VENTAJAS DE LA RED EN MALLA

- Es posible llevar los mensajes de un nodo a otro por diferentes caminos.
- No puede existir absolutamente ninguna interrupción en las comunicaciones.
- Cada servidor tiene sus propias comunicaciones con todos los demás servidores.
- Si falla un cable el otro se hará cargo del tráfico.
- No requiere un nodo o servidor central lo que reduce el mantenimiento.
- Si un nodo desaparece o falla no afecta en absoluto a los demás nodos.
- Si desaparece no afecta tanto a los nodos de redes.

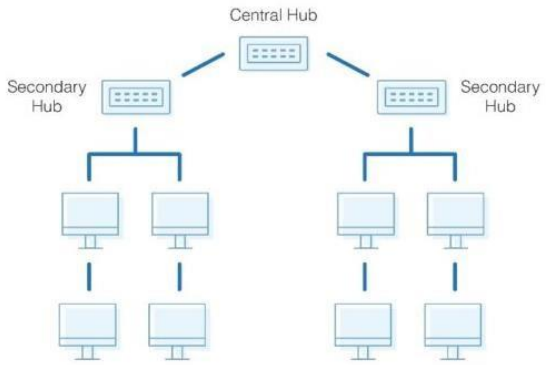
DESVENTAJAS DE LA RED EN MALLA

- El costo de la red puede aumentar en los casos en los que se implemente de forma alámbrica, la topología de red y las características de esta implican el uso de más recursos.
- La disponibilidad del ancho de banda puede verse afectada por la cantidad de usuarios que hacen uso de la red simultáneamente.

Árbol (O jerárquica)

Una red **en árbol** es una de las **más sencillas**, las conexiones entre los nodos están **dispuestas en forma de árbol** con una punta, una base y un nodo de enlace troncal donde se ramifican los demás nodos, el fallo de un nodo **no implica una interrupción** en las comunicaciones, además es fácil la resolución del problema. Uno de los problemas es que **los datos** son recibidos **por todas las**

estaciones sin importar a quien vaya dirigido, esto hace que **no sea muy fiable** y además si se llegara a **desconectar un nodo** todos los que están conectados a él **se desconectaran**.



VENTAJAS DE LA RED EN ÁRBOL

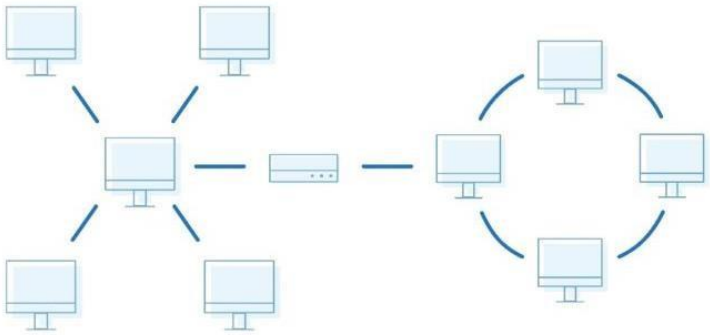
- Permite priorizar las comunicaciones de distintas computadoras.
- Se permite conectar más dispositivos gracias a la inclusión de concentradores secundarios.
- Permite priorizar y aislar las comunicaciones de distintas computadoras.
- Cableado punto a punto para segmentos individuales.
- Soportado por multitud de vendedores de software y de hardware.
- Facilidad de resolución de problemas.
- Mucho más rápida que otra.

DESVENTAJAS DE LA RED EN ÁRBOL

- Si se llegara a desconectar un nodo, todos los que están conectados a él se desconectan también.
- Se requiere más cable.
- La medida de cada segmento viene determinada por el tipo de cable utilizado.
- Es más difícil su configuración.
- Si se viene abajo el segmento principal todo el segmento se viene abajo con él.

Híbrida (Combinada o mixta)

Como su nombre lo indica, es **una combinación de dos o más topologías de red**, para adaptar la red a las necesidades del cliente, de esta manera podemos obtener **infinitas variables de red**. Su implementación se debe a la complejidad de la solución de red o bien al aumento en el número de dispositivos. Este tipo de topologías tienen un **costo muy elevado** debido a su administración y mantenimiento.



VENTAJAS DE LA RED HÍBRIDA

- Combina las ventajas que son propias de cada una de las redes unidas.
- Diagnostica y aísla los fallos de manera eficiente.
- Escanea rápidamente todos los nodos y todos los puntos de hardware para detectar cuando existe un fallo.

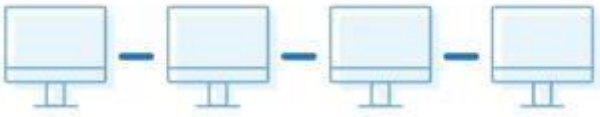
DESVENTAJAS DE LA RED HÍBRIDA

- Tiene un alto costo.
- Difíciles de establecer, extender y resolver cuando se presentan problemas.
- Requiere más cableado entre sus nodos que otros tipos de redes.
- Las inconsistencias y errores en los nodos individuales de una red híbrida son a menudo difíciles de instalar y reparar.
- Requieren puntos o centros inteligentes de concentración.
- Cuando tienen un gran tamaño comúnmente requieren varios concentradores inteligentes.

Margarita

Es la forma **más fácil** de agregar más dispositivos Ethernet a la red. En la red **margarita** una computadora “A” está conectada a otra “B” sin ningún **dispositivo intermedio**, y esa otra, está conectado a otra computadora “C”, y así sucesivamente. Su conexión puede ser lineal o en anillo.

Las conexiones no forman redes, en el ejemplo anterior la computadora “C” **no puede ser conectada directamente** con la computadora “A”.



Ventajas de la red en margarita

- Facilidad de ampliación de la ramas en serie.

DESVENTAJAS DE LA RED EN MARGARITA

- Si el primer elemento de un canal se avería, deja fuera de servicio a los demás.

Lógicas

Medio compartido (O broadcast)

Cada host envía sus datos hacia **todos los demás host** del medio de red, no existe un orden que las estaciones deban seguir para utilizar la red, es por **orden de llegada**. Todos los dispositivos pueden acceder al medio de comunicación compartido en cualquier momento. Funciona bien en redes pequeñas.

Transmisión de token (Basados en token)

Controla el acceso a la red mediante transmisiones de **un token electrónico** a cada host de forma **secuencial** (recorre la red en un orden lógico) Cuando un host **recibe el token**, ese host puede **enviar datos a través de la red**. Si el host no tiene ningún dato para enviar, transmite el token al siguiente host y el proceso se repite. Tiene como desventaja el retardo.

Grado de autentificación

Los grados de autentificación sólo se dividen en **dos tipos**, los cuales son:

Red Privada: una red **privada** se define como una red que puede **usarla solo algunas personas** y que están configuradas con **clave de acceso personal**.

Red de acceso público**:** una red **pública** se define como una red que puede usar **cualquier persona** y no como las redes que están configuradas con clave de acceso personal. Es una red de **computadoras interconectados**, capaz de compartir información y que permite comunicar a usuarios **sin importar su ubicación geográfica**.

Material recopilado del trabajo realizado por los alumnos de Informática General 1er Cuatrimestre 2020

Nombre del grupo	Integrantes
Grupo 1	ABUIN, MATIAS DANIEL (41745291) AIBAR, HERNAN EZEQUIEL (42462359) ALONSO, NICOLAS (37432251) ANIBARRO ALVAREZ, GUSTAVO DANIEL (94234481) ARAGON, YAMILA BELEN (42495417) AVILA, NATALY AGUSTINA (42671687) BARONE, ESTEBAN NICOLAS (43445028) BARRIENTOS, FARID HERNAN (42248355) CABRERA, NOELIA DANIELA ELENA (35603447)
Grupo 2	BARREIRO LUCAS EZEQUIEL (40378915) BIFANO, MARIO (42224895) BONASERA, TOMÁS AGUSTÍN (42720104) BONGIORNO, BRUNO (39769561) BRITO, LEONARDO CIRILO (43509772) CABRERA, ROMINA AYELÉN (40126654) CALERO, DARÍO SEBASTIÁN (43322094) COLOMBA, MALENA (41200999) CORTES, VALERIA NOEMI (40744613)
Grupo 3	CAMPAÑA, JUAN FRANCO (41917617) CARREÑO, IVÁN LAUTARO (43053717) CASTRO, JULIAN EMANUEL (39347169) CHILON CRUZ, EDUAR ROBINZON (94221723) COLMAN, JULIAN (41897557) COLQUE, ALEXIS RUBEN (42999335) DAVIES, MAXIMILIANO NICOLÁS (43309952) DELLA VECCHIA, BIANCA (44162262) ZERPA CONTRERAS, MARIA GABRIELA (96015712)
Grupo 4	FERNANDEZ MELIAN, CRISTIAN HORACIO (41139455) ORUE, VICTOR ADRIAN (38445712) PIESIECKI, LEANDRO NICOLAS (41566607) RAMOS, JUAN MANUEL (40234566) RODRIGUEZ, JONATAN JOEL (41235511) SANCHEZ, KEVIN FABIAN (38428510) VILLEGAS, RODRIGO (40731911) VITERITTI, TOMAS ESTEBAN (42148096)

Grupo 5	DE LA IGLESIA, LUCIANO JAVIER (40536830) DELGADO, CRISTOFER MIGUEL (38913516) DI LAURO, MADELAINE LUDMILA (42093986) DI MARI, AMUYEN (42950543) Douzaklian Saa, Sol (40730374) ESCALERA, ANGEL ALBERTO (42339626) ESCOBAR LASALAS, JOEL CESAR (44107580) ESTEVEZ, LAUTARO NICOLÁS (43718729) TONIETTI, LUCÍA FLORENCIA (44163427)
Grupo 6	CRESPO, ROCIO BELEN (42421309) FERNÁNDEZ MORALES, DANIEL ALBERTO (41708467) FIGUEREDO, ARIANA PAULA (40227993) FILIPPINI LAUTARO IGNACIO (36075122) GARCIA SUAREZ, JULIAN (41428826) GODOY, LUDMILA BELEN (43731094) HERRERA, BRENDA ERIKA FIORELLA (43724139) WAGNER, IAN LAUTARO (40853854)

BIBLIOGRAFIA

Definición de Transmisión de Datos. Madrid, España: Diccionario de Español Jurídico Real Academia Española. Dirección de donde se extrajo el documento https://dej.rae.es/lema/transmisi%C3%B3n-de-datos.
Anónimo. ¿Qué es la Velocidad de Transferencia de Datos? Miami Broward Palm Beach, EEUU: Computer Audio Video Systems Integrator. Dirección de donde se extrajo el documento https://www.cavsi.com/preguntasrespuestas/que-es-la-velocidad-de-transferencia-de-datos/
Anónimo. (20 de Junio 2017). ¿Qué es la comunicación sincrónica y asincrónica en la enseñanza virtual? Cdad. de Guatemala, Guatemala: Galileo Universidad. Dirección de donde se extrajo el documento http://elearningmasters.galileo.edu/2017/06/20/comunicacion-sincronica-y-asincronic
Anónimo. Definición de Velocidad de Transferencia. Sistemas. Dirección de donde se extrajo el documento https://sistemas.com/velocidad-de-transferencia.php
Anónimo. (4 de Mayo del 2016). ¿Cuál es la BER - Bit Error Rate? Distrito de TianHe, GuangZhou, China: Fmuser. Dirección de donde se extrajo el documento https://es.fmuser.net/content/?1906.html
Anónimos AAVV. Conceptos básicos de transmisión de datos. Madrid España: Fiwiki dependiente de alumnos de la Escuela Técnica Superior de Ingenieros Informáticos de la Universidad Politécnica de Madrid. Dirección de donde se extrajo el documento https://www.fiwiki.org/images/f/ff/Tema1.pdf
Ernesto, Luis. Tipos de transmisión de datos. Monografías. Dirección de donde se extrajo el documento https://www.monografias.com/trabajos5/transdat/transdat.shtml
Anónimos AAVV. (25 de Marzo de 2011). Transmisión de datos. Ecuador: EcuRed. Dirección de donde se extrajo el documento https://www.ecured.cu/Transmisi%C3%B3n_de_datos
Anónimos AAVV. (23 de Mayo de 2011). Señales analógicas y digitales. Ecuador: EcuRed. Dirección de donde se extrajo el documento https://www.ecured.cu/index.php?title=Se%C3%B1ales_anal%C3%B3gicas_y_digitales&action=history
Andreotti, Jorge I. (21 de agosto de 2015). ¿Qué es el BER (Bit Error Rate)? Argentina: Ingeniero Andreotti. Dirección de donde se extrajo el documento http://ingenieroandreotti.blogspot.com/2015/08/que-es-el-ber-bit-error-rate_21.html#:~:text=En%20
Anónimo. Medios de transmisión. Málaga, España: HERRAMIENTAS WEB PARA LA ENSEÑANZA DE PROTOCOLOS DE COMUNICACIÓN, Escuela Técnica superior de Ingeniería Informática, Universidad de Málaga (España). Dirección de donde se extrajo el documento http://neo.lcc.uma.es/evirtual/cdd/tutorial/fisico/Mtransm.html

Romero Ternero. María del Carmen. (13 de Julio de 2006). Transmisión de Datos. Sevilla, España: Departamento de Tecnología Electrónica, Universidad de Sevilla. Dirección de donde se extrajo el documento http://www.dte.us.es/personal/mcromero/docs/arc1/tema3-arc1.pdf
Anónimo. (29 de abril de 2020). Transmisión de Datos. Argentina: Facultad de Ciencias Exactas y Naturales Y Agrimensura, Universidad Nacional del Nordeste. Dirección de donde se extrajo el documento http://exa.unne.edu.ar/depar/areas/informatica/teleproc/Comunicaciones/Presentaciones_Proyector/TransmisiondeDatos.pdf
García Arias, Pedro M. (Octubre de 2016). Señales Analógicas y Digitales, Dominio de la Frecuencia y el tiempo, Facultad de Ciencias Matemáticas y Físicas, Universidad de Guayaquil. Guayaquil, Ecuador: Researchgate. Dirección de donde se extrajo el documento https://www.researchgate.net/publication/312587574_Senales_Analogicas_y_Digitales_Dominio_de_la_Frecuencia_y_el_tiempo
Clasificación de redes por alcance
• https://www.gadae.com/blog/tipos-de-redes-informaticas-segun-su-alcance/

Redes de área local
• https://www.ecured.cu/Red_de_%C3%A1rea_local_(LAN)#Comparativa_de_los_tipos_de_redes
• https://es.wikipedia.org/wiki/Red_de_%C3%A1rea_local

Redes de área amplia
• https://concepto.de/red-wan/
• https://www.ticportal.es/glosario-tic/wan-red-area-amplia
• https://www.ionos.es/digitalguide/servidores/know-how/wan/

Red dedicada
• https://es.wikipedia.org/wiki/Red_multipunto#Red_dedicada_o_exclusiva
• https://www.ecured.cu/Redes_punto_a_punto
• https://es.wikipedia.org/wiki/Red_multipunto
• https://www.eninetworks.com/blog-diferencias-entre-el-internet-dedicado-y-otras-conexiones/
• https://www.monografias.com/docs113/lineas-dedicadas/lineas-dedicadas.shtml

Red de área metropolitana
• https://sites.google.com/site/telecomunicacionaa/red-de-area-metropolitana-man
• https://www.monografias.com/trabajos84/redes-man/redes-man.shtml#bibliograa
• https://es.wikipedia.org/wiki/Red_de_%C3%A1rea_metropolitana

Red inalámbrica
• https://es.wikipedia.org/wiki/Red_inal%C3%A1mbrica
• Madrid Molina, J. M. (2006). Seguridad en redes inalámbricas 802.11. http://bibliotecadigital.icesi.edu.co/biblioteca_digital/handle/10906/400

Otros tipos
• https://es.wikipedia.org/wiki/VLAN
• https://www.redeszone.net/2016/11/29/vlans-que-son-tipos-y-para-que-sirven/
• https://www.ionos.es/digitalguide/servidores/know-how/vlan/
• https://es.ccm.net/contents/286-vlan-redes-virtuales
• http://www.alegsa.com.ar/Dic/pan.php
• http://queesunaredpan.blogspot.com/2012/11/v-behaviorurldefaultvmlo.html
• https://www.ionos.es/digitalguide/servidores/know-how/los-tipos-de-redes-mas-conocidos/
• https://www.networkworld.es/networking/que-es-una-san
• https://es.wikipedia.org/wiki/Red_de_área_de_almacenamiento
(2020). Puentes (bridge) - Redes locales y globales. Recuperado de https://sites.google.com/site/redeslocalesyglobales/2-aspectos-fisicos/5-dispositivos-de-interconexion-de-redes/3-puentes

Puentes (Bridges). | ICTV09.- Instalaciones de redes digitales de datos en viviendas y edificios. Ikastaroak.ulhi.net. Obtenido de https://ikastaroak.ulhi.net/edu/es/IEA/ICTV/ICTV09/es_IEA_ICTV09_Contenidos/website_63_puentes_bridges.html

(2017). El Hub o Concentrador. Obtenido de https://camber1redes.wordpress.com/el-hub-o-concentrador/

HUB o concentrador: Qué es, usos en informática y tipos que existen. Profesional Rewiew. Obtenido de https://www.profesionalreview.com/2019/02/12/hub-o-concentrador/

Marcelo Suárez. (2020) ¿Cómo Funciona un Swtich? - CCNA Desde Cero. Obtenido en https://ccnadesdecero.com/curso/como-funciona-un-swtich/

¿Cuál es la diferencia entre el Switch de Capa 2 y el Switch de Capa 3?, (2019). Obtenido en https://community.fs.com/es/blog/layer-2-switch-vs-layer-3-switch-what-is-the-difference.html

Yúbal FM (2018). Cuáles son las diferencias entre Hub, Switch y Router. Obtenido en https://www.xataka.com/basics/cuales-son-las-diferencias-entre-hub-switch-y-router

Dispositivos de Interconexión – ASO. Sitio web Adminso.es. Obtenido en http://www.adminso.es/index.php/3._Dispositivos_de_Interconexi%C3%B3n

Repetidor – EcuRed. Obtenido en https://www.ecured.cu/Repetidor

Router. Obtenido de https://es.wikipedia.org/wiki/Router#Introducci%C3%B3n_a_RIP

Qué es un Switch o conmutador LAN y para qué sirve. Profesional Review. Obtenido en https://www.profesionalreview.com/2020/02/21/switch-conmutador/

5.3.1.2 Tabla de direcciones MAC del switch. Itesa.edu.mx. Obtenido en https://www.itesa.edu.mx/netacad/introduccion/course/module5/5.3.1.2/5.3.1.2.html#:~:text=Cuando%20un%20switch%20recibe%20una,la%20recibi%C3%B3%20en%20primer%20lugar.

Modelo OSI (2020). Recuperado de https://es.wikipedia.org/wiki/Modelo_OSI#cite_note-Nivel_de_transporte-8

SWITCH, HUB, ROUTER, BRIDGE. El Blog de Claudio. Obtenido de https://claudiooq2.wordpress.com/switch-hub-router-bridge/

Valverde (2016). Redes. Obtenido en: https://es.slideshare.net/RandyValverde/clase-4-redes

Gateway (Puerta de enlace). Obtenido en: https://todo-redes.com/equipos-de-redes/gateway-puerta-de-enlace