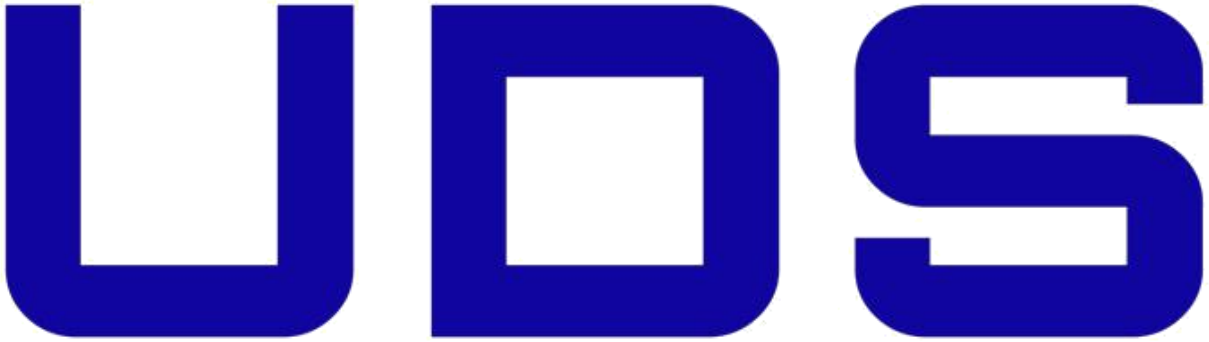


# ANTOLOGIA

*REDES DE COMPUTADORAS I*

*INGENIERIA EN SISTEMAS COMPUTACIONALES*

*5° CUATRIMESTRE*

Enero - Abril

# Marco Estratégico de Referencia

## ANTECEDENTES HISTORICOS

Nuestra Universidad tiene sus antecedentes de formación en el año de 1979 con el inicio de actividades de la normal de educadoras —Edgar Robledo Santiagoll, que en su momento marcó un nuevo rumbo para la educación de Comitán y del estado de Chiapas. Nuestra escuela fue fundada por el Profesor de Primaria Manuel Albores Salazar con la idea de traer Educación a Comitán, ya que esto representaba una forma de apoyar a muchas familias de la región para que siguieran estudiando.

En el año 1984 inicia actividades el CBTiS Moctezuma Ilhuicamina, que fue el primer bachillerato tecnológico particular del estado de Chiapas, manteniendo con esto la visión en grande de traer Educación a nuestro municipio, esta institución fue creada para que la gente que trabajaba por la mañana tuviera la opción de estudiar por las tarde.

La Maestra Martha Ruth Alcázar Mellanes es la madre de los tres integrantes de la familia Albores Alcázar que se fueron integrando poco a poco a la escuela formada por su padre, el Profesor Manuel Albores Salazar; Víctor Manuel Albores Alcázar en septiembre de 1996 como chofer de transporte escolar, Karla Fabiola Albores Alcázar se integró como Profesora en 1998, Martha Patricia Albores Alcázar en el departamento de finanzas en 1999.

En el año 2002, Víctor Manuel Albores Alcázar formó el Grupo Educativo Albores Alcázar S.C. para darle un nuevo rumbo y sentido empresarial al negocio familiar y en el año 2004 funda la Universidad Del Sureste.

La formación de nuestra Universidad se da principalmente porque en Comitán y en toda la región no existía una verdadera oferta Educativa, por lo que se veía urgente la creación de una institución de Educación superior, pero que estuviera a la altura de las exigencias de los jóvenes que tenían intención de seguir estudiando o de los profesionistas para seguir preparándose a través de estudios de posgrado.

Nuestra Universidad inició sus actividades el 18 de agosto del 2004 en las instalaciones de la 4ª avenida oriente sur no. 24, con la licenciatura en Puericultura, contando con dos grupos de

cuarenta alumnos cada uno. En el año 2005 nos trasladamos a nuestras propias instalaciones en la carretera Comitán – Tzimol km. 57 donde actualmente se encuentra el campus Comitán y el Corporativo UDS, este último, es el encargado de estandarizar y controlar todos los procesos operativos y Educativos de los diferentes Campus, Sedes y Centros de Enlace Educativo, así como de crear los diferentes planes estratégicos de expansión de la marca a nivel nacional e internacional.

Nuestra Universidad inició sus actividades el 18 de agosto del 2004 en las instalaciones de la 4ª avenida oriente sur no. 24, con la licenciatura en Puericultura, contando con dos grupos de cuarenta alumnos cada uno. En el año 2005 nos trasladamos a nuestras propias instalaciones en la carretera Comitán – Tzimol km. 57 donde actualmente se encuentra el campus Comitán y el corporativo UDS, este último, es el encargado de estandarizar y controlar todos los procesos operativos y educativos de los diferentes campus, así como de crear los diferentes planes estratégicos de expansión de la marca.

## MISIÓN

Satisfacer la necesidad de Educación que promueva el espíritu emprendedor, aplicando altos estándares de calidad Académica, que propicien el desarrollo de nuestros alumnos, Profesores, colaboradores y la sociedad, a través de la incorporación de tecnologías en el proceso de enseñanza-aprendizaje.

## VISIÓN

Ser la mejor oferta académica en cada región de influencia, y a través de nuestra Plataforma Virtual tener una cobertura Global, con un crecimiento sostenible y las ofertas académicas innovadoras con pertinencia para la sociedad.

## VALORES

- Disciplina
- Honestidad
- Equidad
- Libertad

## ESCUDO

El escudo de la UDS, está constituido por tres líneas curvas que nacen de izquierda a derecha formando los escalones al éxito. En la parte superior está situado un cuadro motivo de la abstracción de la forma de un libro abierto.

## ESLOGAN

—Mi Universidad‖

## ALBORES


Es nuestra mascota, un Jaguar. Su piel es negra y se distingue por ser líder, trabaja en equipo y obtiene lo que desea. El ímpetu, extremo valor y fortaleza son los rasgos que distinguen.

# Mercados Financieros

## Objetivo de la materia:

El objetivo de la asignatura consiste en proporcionar, a los alumnos, los conocimientos teóricos y prácticos necesarios para entender el funcionamiento de los mercados financieros.

Comenzando por una descripción de los mercados en general se pasa, a continuación, al estudio de los mercados monetarios y de capitales, analizando en profundidad el funcionamiento de las Bolsas de Valores. Se analizan los diversos sistemas de contratación bursátil, las OPAs y el crédito al mercado. También se aborda el estudio del mercado de Deuda Pública y el fenómeno de la inversión colectiva.

## Contenido de la Materia

**UNIDAD I**

**INTRODUCCION A LAS REDES**

1.1. Antecedentes históricos.

1.2. Concepto de red.

1.3. Características de la red.

1.4. Que es una red informática.

1.5. Redes de Área Local.

1.6. Componentes de una Red.

1.7. Clasificación de redes.

1.8. Topologías de Redes.

1.9. Dispositivos.

1.10. Intermedios.

1.11. Medios de transmisión.

1.12. Protocolos de comunicación.

## UNIDAD II

## MODELOS DE COMUNICACION

2.1 Conceptos.

2.2 Antecedentes del Modelo OSI.

2.3 Características principales de los niveles del modelo OSI.

2.4 Niveles del modelo OSI.

2.5 Modelos TCP/IP.

2.6 Comparación.

## UNIDAD III

## CAPA DEL MODELO OSI Y TCP/IP

3.1 Niveles del modelo de referencia OSI.

3.2 Transmisión de datos en el modelo OSI

3.3 Modelo de Arquitectura del Protocolo TCP/IP

3.4 Capa de Internet/Red.

3.5 Protocolo UDP

3.6 Datagrama UDP.

3.7 UDP Vs TCP

3.8 Capa de Red.

3.9 IPv4.

3.10 Los Campos de Red y Host y Tipos de dirección IP

## UNIDAD IV

## CAPA DE ENLACE DE DATOS

4.1 Técnica de Control de Acceso al Medio.

4.2 Medios Compartidos.

4.3 Medios no Compartidos.

4.4 Direccionamiento del Control de Acceso al Medio y Tramado de Datos.

4.5 Entandares.

4.6 Comparación entre topologías lógicas y física.

4.7 Señalización y Codificación Física.

4.8 Codificación.

4.9 Medios Guiados.

4.10 Cable Coaxial.

4.11 Fibra Óptica

4.12 Satelites.

# INDICE

## UNIDAD III

## CAPA DEL MODELO OSI Y TCP/IP



## UNIDAD IV

## CAPA DE ENLACE DE DATOS

# UNIDAD I INTRODUCCIÓN A REDES

## 1.1 ANTECEDENTES HISTÓRICOS

Historia de las redes de computadoras.

La historia de las redes de computadoras se puede remontar a 1957 cuando los estados unidos, crearon ARPA (advanced Research Projects Agency), como organismo afiliado al departamento de defensa para impulsar el desarrollo tecnológico. Este organismo procuró fundamentalmente el desarrollo de redes de computadoras y su exponente más significativo Internet.

Un investigador del instituto tecnológico de Massachussets (I.T.M.) de nombre Leonard Kleinrock, escribía el primer libro sobre tecnologías basadas en la transmisión por un mismo cable de más de una comunicación. Estas técnicas se denominan tecnologías de conmutación de paquetes y constituye la base para la transmisión de información entre computadoras.

Un año más tarde de la publicación de Kleinrock 2 científicos del mismo Instituto Tecnológico de Massachussets de nombre Licklinder y Clarck lanzaban la primera publicación (online Man computer Communication; Comunicaciones hombre máquina computadoras en línea) donde se proponía la necesidad de una cooperación social a todos los niveles mediante el uso de redes de computadoras.

Aunque su publicación no tiene un carácter marcadamente científico, si definía las características que deberían tener las comunicaciones en el futuro.

En 1969 se creó la primera red de computadora de la historia esta red se denominó ARPANET y supone el origen de Internet.

La primera comunicación entre dos computadoras se produce entre la UCLA y U. de Stanford el 20 de octubre de 1969.

Inicialmente ARPANET utilizó en NCP (Network Communication Protocolo); protocolo de comunicaciones entre redes, como protocolo base para su funcionamiento.

En ese mismo año la universidad de Michigan crearía una red basada en conmutación de paquetes, con un protocolo X25, se empiezan a editar los primero RFC (Request For Comments) Petición de comentarios. Los RFC, son los documentos que nos normalizan el funcionamiento de las redes de computadoras basadas en TCP/IP, y sus protocolos asociados, estos RFC, explican con detalle como se realizan las comunicaciones, de manera que cualquier fabricante que quiera realizar un protocolo no tiene más que seguir sus instrucciones.

El primer RFC lo editó Steve Crocker (ARPA) el 7 de abril de 1969 y tenía por título (host Software) Software de servidores.

En 1970 ARPANET comienza a utilizare para sus comunicaciones un protocolo host-to-host (máquina a máquina) denominado NCP.

En 1971 la joven ARPANET estaba compuesta por 15 nodos y 23 máquinas que se unían mediante conmutación de paquetes. Ray Tomlinson realiza un programa de correo electrónico para distribuir mensajes a usuarios concretos a través de ARPANET, en ese mismo año cuando se celebra en Washington cuando se celebraba la convención internacional de comunicaciones se realiza el primer CHAT (Conversación interactiva), entre Stanford y BBN, el chat tuvo una consulta médica. En esta misma conferencia se coincide en la necesidad de crear un grupo que profundice en aspectos relativos a las comunicaciones a través de redes de computadoras, y sea real el grupo INVG (INTERNATIONAL NETWORK WORKING GROUP), grupo internacional de trabajo sobre redes de computadoras y fue inicialmente dirigido por Vinton Cerf.

En 1972 se elige el popular signo @ como tecla de puntuación para la separación del nombre del usuario y de la máquina donde estaba dicho usuario.

En 1973 se produce la primera conexión internacional de ARPANET.
Se empieza a tomar en cuenta la importancia de trabajar con redes de computadoras y de generar la creación de JUNET (Japan Unix Network) JANET (Joint Academia network) académica unida en Inglaterra Netnorth (Red del norte), en Canadá el anuncio por parte de la Unión Soviética Anexarse a la Usenet.

1985 Se establecen responsabilidades para el control de los nombres de dominio y así el ISI Instituto de Ciencias para la información, asume la responsabilidad de ser la raíz para la resolución de los nombres de dominio, mientras que el SRI asume la responsabilidad de asignar estos nombres en los que se conoce como registros NIC (Network Information Center) Centro de información de red. El 15 de marzo de 1985, se produce el primer registro de nombre de dominio (Symbolics. Com) a los que seguirías cmu.edu. pudue.edu. rice.edu. UCLA.edu.

En 1986 se crearían la primera red troncal de Internet. Este tipo de grandes redes troncales, que unen multitud de pequeñas redes se denomina Backbones. El nombre del primer Backbone fue NSFNET (Nacional Science Foundation Network) Red de la fundación nacional de ciencias; tenía un ancho de banda de 56000 bits por segundo y unía 5 centros de supercomputadoras.

A partir de 1987 han sucedido numerosos acontecimientos que han convertido a las redes de computadoras en general y a Internet en particular, en una nueva revolución cultural que ha afectado prácticamente todas las facetas de la vida cotidiana, su impacto hoy en día es indiscutible en los albores del siglo XXI, la sociedad de la información presenta como alternativa real muchas pautas de comportamiento desarrolladas sobre el siglo XX que han tenido que redefinir su forma de ver y entender las cosas.

## 1.2 CONCEPTO DE RED

Una red de comunicación o de telecomunicaciones (comunicación remota), es el conjunto de infraestructura, medios de almacenamiento (disco, etc.) y equipamiento de hardware o software que permiten enlazar las terminales entre sí y transferir los datos desde una fuente hacia los destinatarios.

## 1.3 CARACTERÍSTICAS DE RED

Mediante el análisis del sistema de una comunicación telefónica, usted podrá comprender con rapidez los elementos esenciales de la comunicación. Así cualquier tipo de comunicación se distingue cuatro elementos básicos:
El mensaje que se ha de transmitir
Un emisor
Un receptor
Un canal de comunicación.

Este mensaje deberá ser comprensible y capaz de poder detectar algún error en la transmisión.

El mensaje constituye el primer elemento de la comunicación entre dos entidades, el cual puede revertirse de varias formas y con una duración, variable. Los tipos de mensajes de transmisión de datos incluyen los archivos, las solicitudes de servicios y las redes puestas en las mismas, los informes sobre los estados de los dispositivos o de las redes, el control de estas informaciones y un medio de correspondencia como el correo electrónico, el emisor, la fuente de origen al mensaje. El emisor puede ser una persona, una aplicación o una máquina dotada de una "inteligencia" capaz de elaborar un mensaje o proporcionar una respuesta sin que haya intervención humana alguna.

El receptor es destino al cual va dirigido el mensaje, puede ser un computador, una terminar una impresora remota, una persona u otro medio como el teléfono, un aparato de aire acondicionado, etc. Si hubiera un emisor y un mensaje pero se carecería de un receptor, la comunicación no se realizaría. Por ejemplo, si se envían señales con la intención de entrar en contacto con otros tipos de inteligencia, pero no hay nadie que las reciba, la comunicación no se llevará acabo. En una red de área local es posible enviar un mensaje a todos los nodos para indicar que se ofrece una nueva opción; pero si todos los nodos están desactivados en el momento del envío la comunicación se invalidará.

Por último, es factible utilizar varios canales para transmitir el mensaje del emisor al receptor. Por ejemplo, en una comunicación de voz las ondas del sonido viajan por el aire (el canal). En el caso de las redes locales estas se transmiten los datos a través de medios de comunicación, como los cables coaxiales, las ondas infrarrojas, etc.

Por otro lado, la comunicación, no se logra si el mensaje no se comprende de forma correcta, a pesar de que cuente con los cuatro elementos mencionados antes. Así, las diferencias idiomáticas constituyen el principal obstáculo de la comprensión de un mensaje surgido de la comunicación humana, lo cual fundamenta la existencia de intérpretes y traductores. Este mismo problema se presenta en el mundo de las comunicaciones computacionales.

Por tanto, los datos se pueden transmitir en uno de los diferentes códigos, aunque los más comunes son el código estándar americano para el intercambio de información (ASCII) y el código extendido de intercambio de decimales codificado en binario (EBCDIC), en 256 caracteres.

## 1.4 ¿QUÉ ES UNA REDINFORMÁTICA?

Es el conjunto de técnicas, conexiones físicas y programas informáticos empleados para conectar 2 o más ordenadores o computadoras. Los usuarios de una red pueden compartir ficheros, impresoras y otros recursos. Enviar mensajes electrónicos y ejecutar programas en otros ordenadores.

Redes de computadoras. Las redes están formadas por conexiones entre grupos de computadoras y dispositivos asociados, que permiten a los usuarios la transferencia electrónica de información.

Las diferentes computadoras se denominan estaciones de trabajo y se comunican entre sí a través de un cable o línea telefónica conectada a los servidores. Estas son computadoras como las estaciones de trabajo pero poseen funciones administrativas y están dedicados exclusiva a supervisar el acceso de las estaciones de trabajo a la red y a los recursos compartidos (como las impresoras). Por ello cabe hacer mención que al utilizar un MODEM este esta permitiendo a las computadoras transmitir información a través de una línea telefónica normal. El MODEM transmite las señales digitales a analógicas e inversa y permite la comunicación entre computadoras muy distantes entre sí. Una red tiene tres niveles de componentes:

1.-. Software de aplicación
2.- Software de Red
3.- Hardware de Red

El software de aplicación, esta formado por programas informáticos que se comunican con los usuarios de la red y permiten compartir información (Como archivos de bases de datos, de documentos, datos, gráficos o videos) y recursos (como impresoras o unidades de disco) un tipo de software de aplicaciones se denomina cliente servidor. Las computadoras cliente envían peticiones de información o de uso de recursos a otra computadora, llamadas servidores, que controlan el flujo de datos y la ejecución de las aplicaciones, a través de la red. Otro tipo de software de aplicación se conoce como" de igual a igual" o de (peer to

peer) en una red de este tipo, los ordenadores se envían entre sí mensajes y peticiones directamente si utilizan un servidor como intermediario. Estas redes son mas restringidas en sus capacidades de seguridad, auditoria y control normalmente se utiliza en ámbitos de trabajo con pocos ordenadores en los que no se precisa un control tan estricto del uso de aplicaciones y privilegios para el acceso y modificación de datos: Se utilizan, por ejemplo: En redes domésticas o en grupos de trabajo dentro de una red corporativa más amplia.

## 1.5 REDES DE ÁREA LOCAL

Las redes de área local (generalmente conocidas como LANs) son redes de propiedad privada que se encuentran en un solo edificio o en un campus de pocos kilómetros de longitud. Se utilizan ampliamente para conectar computadoras personales y estaciones de trabajo en oficinas de una empresa y de fábricas para compartir recursos (por ejemplo, impresoras) e intercambiar información.

Las LANs son diferentes de otros tipos de redes en tres aspectos 1) Tamaño, *2)* Tecnología de transmisión y *3)* topología.

Las LANs están restringidas por tamaño, es decir, el tiempo de transmisión en el peor de los casos es limitado y conocido de antemano. El hecho de conocer este límite permite utilizar ciertos tipos de diseño, lo cual no sería posible de otra manera. Esto también simplifica la administración de la red.

## 1.6 COMPONENTES DE UNA RED

Actualmente las redes de computadoras son un elemento fundaméntala en casi todas las actividades que se realizan en el ámbito, personal, académico y laboral, la mayoría de las personas no reflexiona en como operan estas redes y solo les interesa la velocidad y estabilidad que tenga.

Como parte del proceso de aprendizaje de informática es necesario conocer los elementos básicos de Software y Hardware que permiten hacer llegar los datos a los diversos dispositivos de una red así como el aprender a manipularlos para hacer más eficientes, rápidas y obtener como informáticos el mayor provecho a los dispositivos conectados a la red.

Para dar inicio a la comprensión de una red, se encuentra este video en internet, el sonido es malo pero contiene la información básica para entender que es una red.

Una vez comprendido lo básico de una red, a continuación se nombran algunos tipos de red y la manera en la que pueden ser utilizados.

**Componenetes de una RED**

**Servidor.-** Es una computadora que, formando parte de una red, provee servicios a otras computadoras denominadas clientes. También se suele denominar con la palabra servidor a Una aplicación informática o programa que realiza algunas tareas en beneficio de otras aplicaciones llamadas clientes. Algunos servicios habituales son los servicios de archivos, que permiten a los usuarios almacenar y acceder a los archivos de una computadora y los servicios de aplicaciones, que realizan tareas en beneficio directo del usuario final.

**Estaciones de Trabajo**.- Cuando una computadora se conecta a una red, la primera se convierte en un nodo de la última y se puede tratar como una estación de trabajo o cliente.

Las estaciones de trabajos pueden ser computadoras personales, se encargan de sus propias tareas de procesamiento, así que cuanto mayor y más rápido sea el equipo, mejor.

**Tarjeta de conexión a la red**.- Toda computadora que se conecta a una red necesita de una tarjeta de interfaz de red que soporte un esquema de red especifico, como Ethernet, ArcNet o Token Ring. El cable de red se conectara a la parte trasera de la tarjeta, la compatibilidad a nivel físico y lógico se convierte en una cuestión relevante cuando se considera el uso de cualquier tarjeta de red. Hay que asegurarse que la tarjeta pueda funcionar en la estación deseada, y de que existen programas controladores que permitan al sistema operativo enlazarlo con sus protocolos y características a nivel físico.

**Repetidores.-** Es un dispositivo electrónico que recibe una señal débil o de bajo nivel y la retransmite a una potencia o nivel más alto, de tal modo que se puedan cubrir distancias más

largas sin degradación o con una degradación tolerable. El término repetidor se creó con la telegrafía y se refería a un dispositivo electromecánico utilizado para regenerar las señales telegráficas. El uso del término ha continuado en telefonía y transmisión de datos.

**Bridges**.- Es un dispositivo de interconexión de redes de ordenadores que opera en la capa 2 (nivel de enlace de datos) del modelo OSI. Este interconecta dos segmentos de red (o divide una red en segmentos) haciendo el pasaje de datos de una red hacia otra, con base en la dirección física de destino de cada paquete.

Un bridge conecta dos segmentos de red como una sola red usando el mismo protocolo de establecimiento de red, la principal diferencia entre un bridge y un hub es que el segundo pasa cualquier trama con cualquier destino para todos los otros nodos conectados, en cambio el primero sólo pasa las tramas pertenecientes a cada segmento. Esta característica mejora el rendimiento de las redes al disminuir el tráfico inútil.

Para hacer el bridging o interconexión de más de 2 redes, se utilizan los switch.

Se distinguen dos tipos de bridge:

**Locales**: sirven para enlazar directamente dos redes físicamente cercanas.

**Remotos o de área extensa**: se conectan en parejas, enlazando dos o más redes locales, formando una red de área extensa, a través de líneas telefónicas y/o de algún otro tipo de interconexión.

Funciona a través de una tabla de direcciones MAC detectadas en cada segmento a que está conectado. Cuando detecta que un nodo de uno de los segmentos está intentando transmitir datos a un nodo del otro, el bridge copia la trama para la otra subred. Por utilizar este

mecanismo de aprendizaje automático, los bridges no necesitan configuración manual.

Actualmente es poco frecuente tener Bridges como unidades independientes y más bien se encuentran integrados a los Routers (que se mencionan más delante) en una sola unidad que en ocasiones se denomina Brouter (Bridge+Router).

**Hubs**.- es un dispositivo que permite centralizar el cableado de una red y poder ampliarla. Esto significa que dicho dispositivo recibe una señal y repite esta señal emitiéndola por sus diferentes puertos.

Funciona repitiendo cada paquete de datos en cada uno de los puertos con los que cuenta, excepto en el que ha recibido el paquete, de forma que todos los puntos tienen acceso a los datos. También se encarga de enviar una señal de choque a todos los puertos si detecta una colisión, son la base para las redes de topología tipo estrella, existen 3 clases.

Pasivo.- No necesita energía eléctrica. Se dedica a la interconexión.

Activo.- Necesita alimentación. Además de concentrar el cableado, regeneran la señal, eliminan el ruido y amplifican la señal

Inteligente.-También llamados Smart hubs son hubs activos que incluyen microprocesador.

Físicamente son muy parecidos a los Switchers (que se verá a continuación) además de que sus funciones son muy similares,

**Hub**

**Switch**.- Es un dispositivo digital de lógica de interconexión de redes de computadores que opera en la capa 2 (nivel de enlace de datos) del modelo OSI. Su función es interconectar dos o más segmentos de red, de manera similar a los puentes (bridges), pasando datos de un segmento a otro de acuerdo con la dirección MAC de destino de las tramas en la red.

**Routers**.- Es un enrutador, elemento que marca el camino mas adecuado para la transmisión de mensajes en una red completa, este toma el mejor camino para enviar los datos dependiendo del tipo de protocolo que este cargado, cuenta con un procesador es el mas robusto, tiene mas procesadores y mucha mas capacidad en sus respectivas memorias, Sus características esenciales son

Es un dispositivo Inteligente
Procesa y toma decisiones

Genera tabla de enrutamiento (conoce si sus Routers vecinos están en funcionamiento).
Siempre toma una dirección Lógica.
Tiene varias interfaces (sirven para interconectarse con las redes LAN u otros Routers). Reconoce las redes que tiene directamente conectadas
Mantiene una actualización constante de la topología (depende del protocolo).
LOAD 1/255 entre menor sea el numerador esta mas ocupado.
RALY 255/255 entre mayor sea el numerador es mas confiable y seguro.

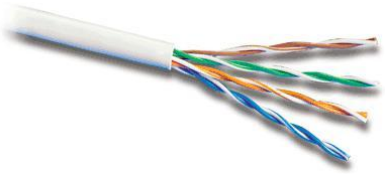
**Brouters**.- Es un dispositivo de interconexión de redes de computadores que funciona como un bridge (puente de red) y como un enrutador. Un brouter puede ser configurado para actuar como bridge para parte del tráfico de red, y como enrutador para el resto.


**Firewall** .- Es un elemento de seguridad que filtra el tráfico de red que a él llega, con un cortafuegos se puede aislar un ordenador de todos los otros ordenadores de la red excepto de uno o varios que son los que nos interesa que puedan comunicarse con él.


**Cableado**.- Los tipos de cableado de red más populares son: par trenzado, cable coaxial y fibra óptica, además se pueden realizar conexiones a través de radio o microondas, dependiendo el tipo de red y los requerimientos de la misma, velocidad y longitud se debe considerar el tipo de cable a utilizar

Par Trenzado.- Consiste en dos hilos de cobre trenzado, aislados de forma independiente y trenzados entre sí. El par está cubierto por una capa aislante externa. Entre sus principales ventajas tenemos:

Es una tecnología bien estudiada
No requiere una habilidad especial para
instalación La instalación es rápida y fácil
La emisión de señales al exterior es mínima.
Ofrece alguna inmunidad frente a interferencias, modulación cruzada y corrosión.



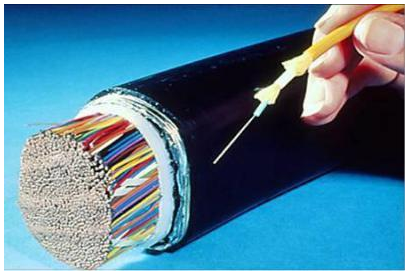
Cable Coaxial.- Se compone de un hilo conductor de cobre envuelto por una malla trenzada plana que hace las funciones de tierra. entre el hilo conductor y la malla hay una capa gruesa de material aislante, y todo el conjunto está protegido por una cobertura externa, está disponible en dos espesores: grueso y fino.

El cable grueso soporta largas distancias, pero es más caro, el cable fino puede ser más práctico para conectar puntos cercanos, el cable coaxial ofrece las siguientes ventajas:

Soporta comunicaciones en banda ancha y en banda base.
Es útil para varias señales, incluyendo voz, video y datos.
Es una tecnología bien estudiada.

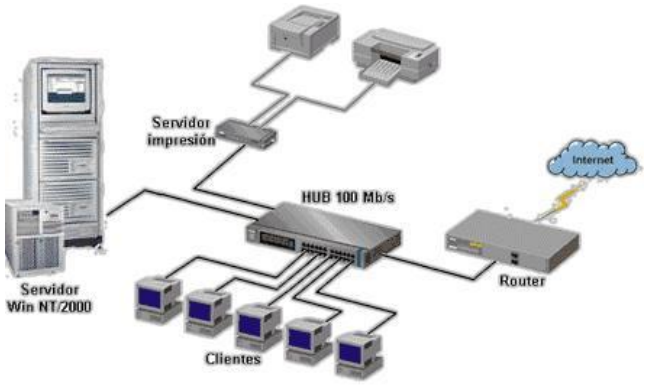
Conexión fibra óptica.- Esta conexión es cara, permite transmitir la información a gran velocidad e impide la intervención de las líneas, como la señal es transmitida a través de luz, existen muy pocas posibilidades de interferencias eléctrica o emisión de señal, el cable consta de dos núcleos ópticos, uno interno y otro externo, que refractan la luz de forma distinta. La fibra está encapsulada en un cable protector , ofrece las siguientes ventajas:

Alta velocidad de transmisión
No emite señales eléctricas o magnéticas, lo cual redunda en la seguridad
Inmunidad frente a interferencias y modulación cruzada. Mayor economía que el cable coaxial en algunas instalaciones.
Soporta mayores distancias



**Software**.- :En el software de red se incluyen programas relacionados con la interconexión de equipos informáticos, es decir, programas necesarios para que las redes de computadoras funcionen. Entre otras cosas, los programas de red hacen posible la comunicación entre las

computadoras, permiten compartir recursos (software y hardware) y ayudan a controlar la seguridad de dichos recursos.




**Sistema operativo de red** .- Después de cumplir todos los requerimientos de hardware para instalar una RED, se necesita instalar un sistema operativo de red (Network Operating System, NOS), que administre y coordine todas las operaciones de dicha red.Los sistemas operativos de red tienen una gran variedad de formas y tamaños,debido a que cada organización que los emplea tiene diferentes necesidades. Algunos sistemas operativos se comportan excelentemente en redespequeñas, así como otros se especializan en conectar muchas redes pequeñasen áreas bastante amplias.

Los servicios que el NOS realiza son:

Soporte para archivos.- Esto es, crear, compartir, almacenar y recuperar archivos, actividades esenciales en que el NOS se especializa proporcionandoun método rápido y seguro.

Comunicaciones.- Se refiere a todo lo que se envía a través del cable, la comunicación se realiza cuando por ejemplo, alguien entra a la red, copia unarchivo, envía correo electrónico, o imprime.

Servicios para el soporte de equipo.- Aquí se incluyen todos los serviciosespeciales como impresiones, respaldos en cinta, detección de virus en la red,etc.

## Tipos de Redes

Las redes según sea la utilización por parte de los usuarios puede ser: compartida o exclusiva.

**Redes dedicadas o exclusivas.-**Son aquellas que por motivo de seguridad, velocidad o ausencia de otro tipo de red, conectan dos o más puntos de forma exclusiva. Este tipo de red puede estructurarse en redes punto a punto o redes multipunto.

**Redes punto a punto**.- Permiten la conexión en línea directa entre terminales y computadoras. la ventaja de este tipo de conexión se encuentra en la alta velocidad de transmisión y la seguridad que presenta al no existir conexión con otros usuarios. Su desventaja sería el precio muy elevado de este tipo de red.

**Redes multipunto.**- Permite la unión de varios terminales a su correspondiente computadora compartiendo una única línea de transmisión. La ventaja consiste en el abaratamiento de su costo, aunque pierde velocidad y seguridad, este tipo de redes requiere amplificadores y difusores de señal o de multiplexores que permiten compartir líneas dedicadas.

**Redes compartidas** .- Son aquellas a las que se une un gran número de usuarios, compartiendo todas las necesidades de transmisión e incluso con transmisiones de otras naturalezas. Las redes más usuales son las de conmutación de paquetes y las de conmutación de circuitos.

**Redes de conmutación de paquetes**.- Son redes en las que existen nodos de concentración con procesadores que regulan el tráfico de paquetes.

**Redes de conmutación de circuitos**.- Son redes en las que los centros de conmutación establecen un circuito dedicado entre dos estaciones que se comunican.

**Redes digitales de servicios integrados(RDSI)**.- Se basan en desarrollos tecnológicos de conmutación y transmisión digital. La RDSI es una red totalmente digital de uso general capaz de integrar una gran gama de servicios como son la voz, datos, imagen y texto, la RDSI requiere de la instalación de centrales digitales.

Las redes según los servicios que satisfacen a los usuarios se clasifican en:

**Redes para servicios básicos de transmisión**.- Se caracterizan por dar servicio sin alterar la información que transmiten. De este tipo son las redes dedicadas, la red telefónica y las redes de conmutación de circuitos.

**Redes para servicios de valor añadido**.- Son aquellas que además de realizar la transmisión de información, actúan sobre ella de algún modo, pertenecen a este tipo de red: las redes que gestionan mensajería, transferencia electrónica de fondos, acceso a grandes bases de datos, videotex, teletex, etc.

*Nota:*

***Paquete**.- Es una pequeña parte de la información que cada usuario desea transmitir. Cada paquete se compone de la información, el identificador del destino y algunos caracteres de control.*

Para poder instalar y administrar una red es necesario entender sus componentes los cuales se dividen en Hardware y Software.

## 1.7 CLASIFICACIÓN DE REDES.

Las redes de computadoras se clasifican por su tamaño, es decir la extensión física en que se ubican sus componentes, desde un aula hasta una ciudad, un país o incluso el planeta. Dicha clasificación determinará los medios físicos y protocolos requeridos para su operación, por ello se han definido tres tipos:

**Redes de Área Local o LAN (Local Área Network).**

Permiten la interconexión desde unas pocas hasta miles de computadoras en la misma área de trabajo como por ejemplo un edificio. Son las redes más pequeñas que abarcan de unos pocos metros a unos pocos kilómetros.

**Redes de Área Metropolitana o MAN (Metropolitan Área Network).**

Tiene cubrimiento en ciudades enteras o partes de las mismas. Su uso se encuentra concentrado en entidades de servicios públicos como bancos.

**Redes de Área Amplia o WAN (Wide Área Network)**.

Esta cubre áreas de trabajo dispersas en un país o varios países o continentes. Para lograr esto se necesitan distintos tipos de medios: satélites, cables interoceánicos, radio, etc. Así como la infraestructura telefónica de larga distancias existen en ciudades y países, tanto de carácter público como privado.

**¿Cómo es el funcionamiento de una red de área local?**

Esta red permite la comunicación de las estaciones de trabajo entre sí y el Servidor (y los recursos asociados a él); para dicho fin se utiliza un sistema operativo de red que se encarga de la administración de los recursos como así también la seguridad y control de acceso al sistema interactuando con el sistema operacional de las estaciones de trabajo. El usuario hace una petición a una opción específica desde el sistema operacional de la estación de trabajo, y si este a necesitar un recurso de la red transfiere control al software de la red.

La conexión de las computadoras y dispositivos de la red, se hace generalmente con cables de par trenzado o coaxial pudiendo obtener velocidades de trasmisión entre 1, 10 y 100 Mb hasta los Gigabit por segundo.

**De acuerdo a su relación.**

**Existen 2 tipos:**

**Cliente - Servidor:** Existe un conjunto de computadoras de las cuales hay una que se le llama Servidor encargada de administrar los recursos, dar servicios y compartir información con las demás computadoras llamadas Clientes. Ejemplo: Servidor de Hotmail (correo electrónico).

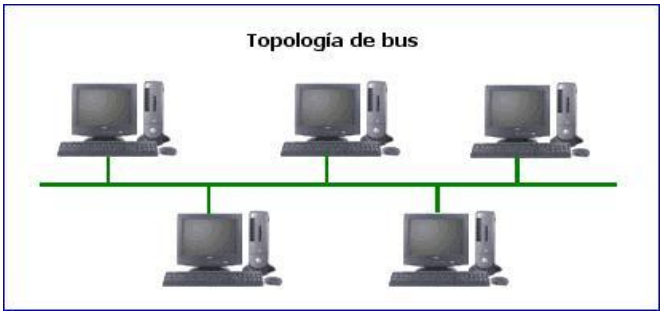
**Peer to Peer:** Todos o algunos aspectos de la red funcionan sin clientes ni servidores fijos, sino una serie de nodos que se comportan como iguales entre sí. Es decir, actúan simultáneamente como clientes y servidores respecto a los demás nodos de la red. Ejemplo: LimeWire (permite compartir diferentes archivos).

## 1.8 TOPOLOGÍAS DE REDES: FÍSICAS Y LÓGICAS.

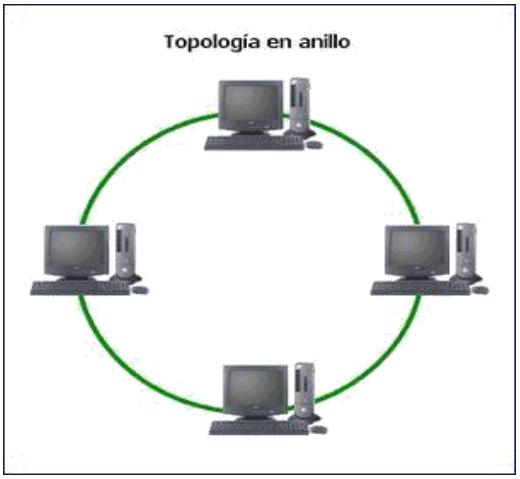
### Topología Física

Consiste en la configuración o disposición del cableado y equipos de comunicación. Entre ellas están:

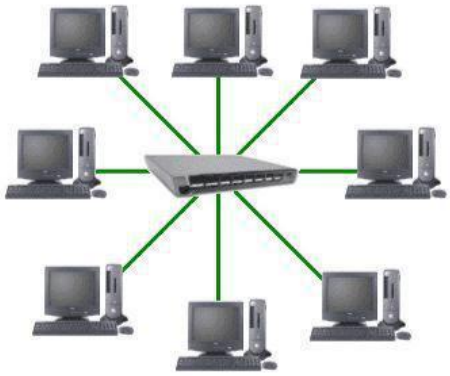
**Bus:** utilizan un troncal único, todos los nodos se conectan directamente a éste y comparten el medio.




**Anillo:** Un nodo se conecta al próximo y el último al primero.



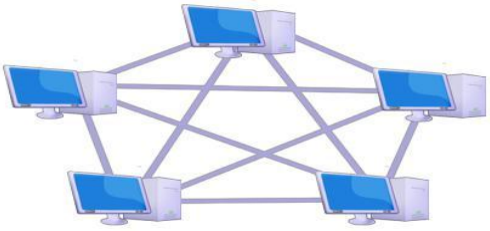

**Estrella:** Todos los nodos se trasmiten a un punto central común, usualmente es un hub o switch.



**Estrella Extendida:** Enlaza las estrellas conectadas a los switches de estas a un swith central.

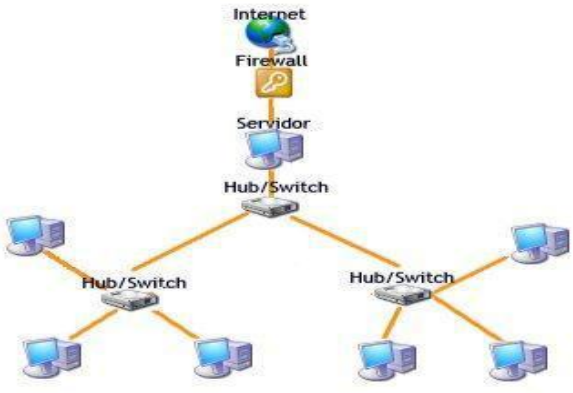
Topologia en estrella extendida

**Topología de Mallas:** Cada host es conectado a todos los otros. Existen múltiples caminos de un nodo a otro. Utilizadas generalmente donde se requiere que no haya interrupciones en la comunicación de un nodo a otro.



Topologia en malla

**Topología de Árbol:** La topología de árbol combina características de la topología de estrella con la BUS. Consiste en un conjunto de subredes estrella conectadas a un BUS. Esta topología facilita el crecimiento de la red.



**Topologías Lógicas**

Ethernet: Cada host envía sus datos a todos los otros host conectados al medio físico en la red. No hay un orden de trasmisión de datos, el primero en acceder al medio es el primero en transmitir.

Token Ring: Aquí se controla el acceso al medio utilizando un testigo electrónico que se pasa a cada host. Cuando un host recibe el testigo puede transmitir datos si los tiene. Si no, entonces pasa el testigo al siguiente host.

## 1.9 DISPOSITIVOS

Un dispositivo de interconexión de redes, es un término ampliamente utilizado para cualquier Hardware que conecte diferentes recursos de red. Los dispositivos claves que comprenden una red son conmutadores, enrutadores, rigde (puentes), repetidores y puertas de enlace.

## 1.10 INTERMEDIOS

Los equipos intermedios son nodos de conexión que se colocan entre los equipos finales o terminales y tienen como función repetir la señal, enrutador paquete de información entre las distintas redes y hacer de concentración entre dispositivos de la red.

## 1.11 MEDIOS DE TRANSMISIÓN

Dentro de los medios de transmisión guiados, los más utilizados en el campo de las telecomunicaciones y la inter conexión de computadoras son tres: cable de par trenzado, cable coaxial y fibra óptica.

## 1.12 PROTOCOLOS DE COMUNICACIÓN

Conjunto de reglas, además son los estándares y políticas formales, conformados por restricciones, procedimientos y formatos que definen el intercambio de paquetes de información para lograr la comunicación entre dos servidores o mas dispositivos a través de una red.

# UNIDAD II

# MODELOS DE COMUNICACIÓN

## 2.1 CONCEPTOS

Una red de computadoras, también llamada red de ordenadores, red de comunicaciones de datos o red informática, es un conjunto de equipos informáticos y software conectados entre sí por medio de dispositivos físicos que envían y reciben impulsos eléctricos, ondas electromagnéticas o cualquier otro medio para el transporte de datos, con la finalidad de compartir información, recursos y ofrecer servicios, es aquí donde se consideran los modelos de comunicación.

Se conoce como familia de protocolos de Internet al conjunto de protocolos que son implementados por la pila de protocolos sobre los cuales se fundamenta Internet y que permiten la transmisión de datos entre las redes de computadoras.

Los dos protocolos más importantes y que fueron también los primeros en definirse y en ser utilizados son: TCP (Protocolo de Control de Transmisión o Transmission Control Protocol) e IP (Protocolo de Internet o Internet Protocol), de ahí que el modelo se denomine como TCP/IP. Los protocolos existentes superan los cien, ente los cuales podemos mencionar como los más conocidos a HTTP, FTP, SMTP, POP, ARP, entre otros. TCP/IP es la plataforma que sostiene Internet y que permite la comunicación entre dos equipos, no

importando si estos cuentan con diferentes sistemas operativos, ya sea sobre redes de área local (LAN) o redes de área extensa (WAN).

El modelo TCP/IP es un protocolo dirigido a la transferencia de información a través de internet, o, dicho de otra manera, es un protocolo utilizado por todas las computadoras conectadas a una red, de manera que estos puedan comunicarse entre sí.

Por otro lado, el modelo OSI ha servido como fundamento teórico para la interconexión de sistemas abiertos, basándose en un conjunto de siete capas. Cada capa cumple funciones específicas requeridas para comunicar dos sistemas mediante una estructura jerárquica. Cualquiera de sus siete capas se apoya en la capa anterior, realiza su función y ofrece un servicio a la capa superior. De acuerdo con, este modelo posee la ventaja de poder cambiar una capa sin necesidad de.

## 2.2 ANTECEDENTES DEL MODELO OSI

El desarrollo de las redes informáticas y su expansión a inicios de la década de 1980 arrojó la necesidad de interconectar los sistemas provenientes de diversos orígenes, o las redes que estos formaban y mantenían. Como ocurre con las personas que hablan idiomas diferentes, las telecomunicaciones se veían imposibilitadas de continuar su ruta expansiva.

Incluso los programas diseñados para la interconexión tenían problemas entre sí, ya que las normas de copyright sobre el diseño computarizado suponían una barrera adicional.

La idea de crear el Modelo OSI como solución a este problema surgió luego de que la ISO llevara a cabo una investigación en la materia. Así, ISO se propuso determinar el conjunto general de reglas aplicables a todas las redes.

### ¿Cómo funciona el modelo OSI?

El funcionamiento del Modelo OSI depende directamente de sus siete capas, en las que descompone el complicado proceso de la comunicación digital. Al compartimentarlo, asigna a cada capa funciones muy específicas, dentro de una estructura jerárquica fija.

Así, cada protocolo de comunicación emplea estas capas en su totalidad o sólo algunas de ellas, pero al obedecer este conjunto de reglas, garantiza que la comunicación entre las redes sea eficaz y sobre todo que se de en los mismos términos.

### ¿Para qué sirve el modelo OSI?

El Modelo OSI es fundamentalmente una herramienta conceptual, de organización de las telecomunicaciones. Universaliza la manera en que la información es compartida entre redes informáticas o sistemas computarizados, independientemente de su origen geográfico, empresarial u otras condiciones que podrían dificultar la comunicación de los datos.

El Modelo OSI no es una topología de red, ni un modelo de red en sí mismo, ni una especificación de protocolos; simplemente es una herramienta que define la funcionalidad de los protocolos, para conseguir un estándar de comunicación, o sea, lograr que todos los sistemas hablen el mismo idioma. Sin él, una red tan vasta y variopinta como Internet sería prácticamente imposible.

## 2.3 CARACTERÍSTICAS PRINCIPALES DE LOS NIVELES DEL MODELO OSI

El modelo OSI se basa en una propuesta que desarrolló la Organización Internacional de Normas, la ISO, como primer paso hacia la estandarización internacional de los protocolos que se usan en las diversas capas. El modelo se llama **modelo de referencia OSI de la ISO**, puesto que se ocupa de la conexión de sistemas abiertos, es decir, sistemas que están abiertos a la comunicación con otros sistemas.

El modelo OSI tiene siete capas. Los principios que se aplicaron para llegar a las siete capas son los siguientes:

1. Se debe crear una capa siempre que se necesite un nivel diferente de abstracción.

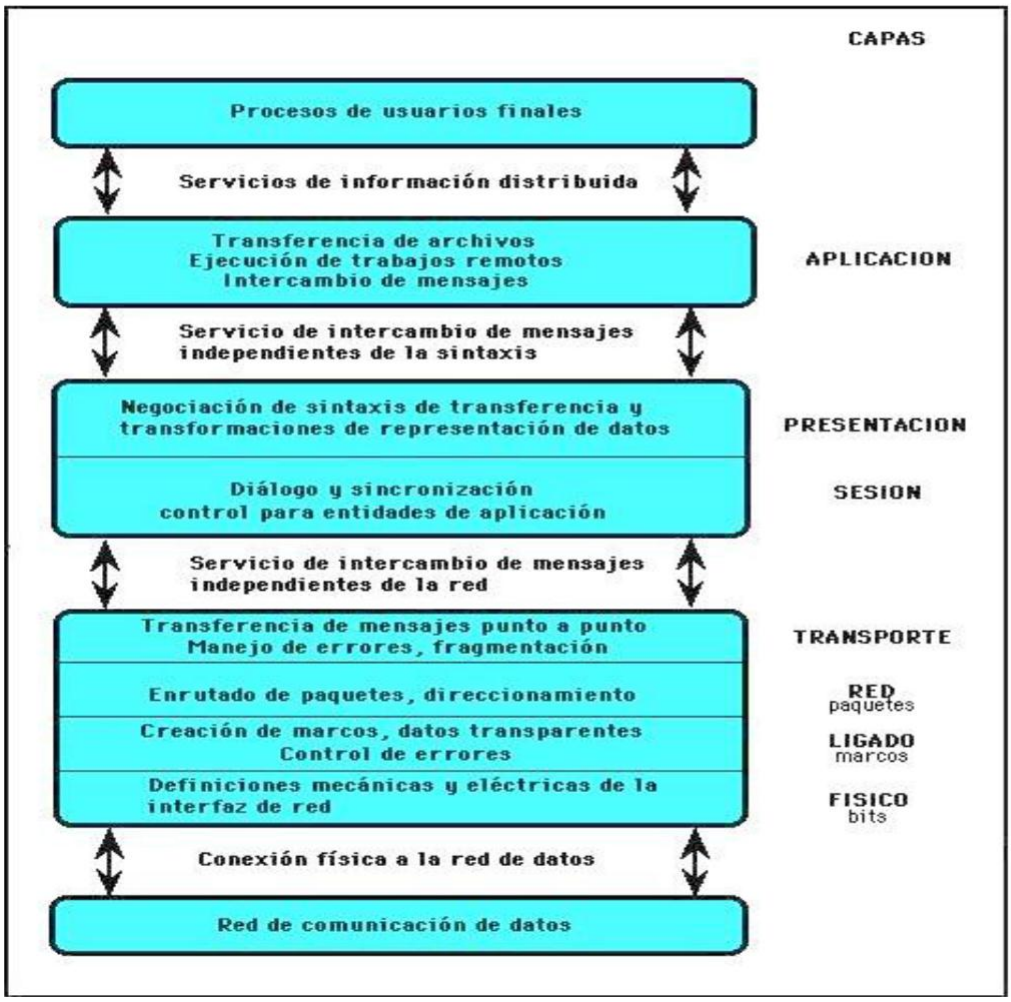
2. Cada capa debe realizar una función bien definida.

La función de cada capa se debe elegir pensando en la definición de protocolos estandarizada internacionalmente.

3. Los límites de las capas deben elegirse a modo de minimizar el flujo de información a través de las interfaces.

4. La cantidad de capas debe ser suficiente para no tener que agrupar funciones distintas en la misma capa y lo bastante pequeña para que la arquitectura no se

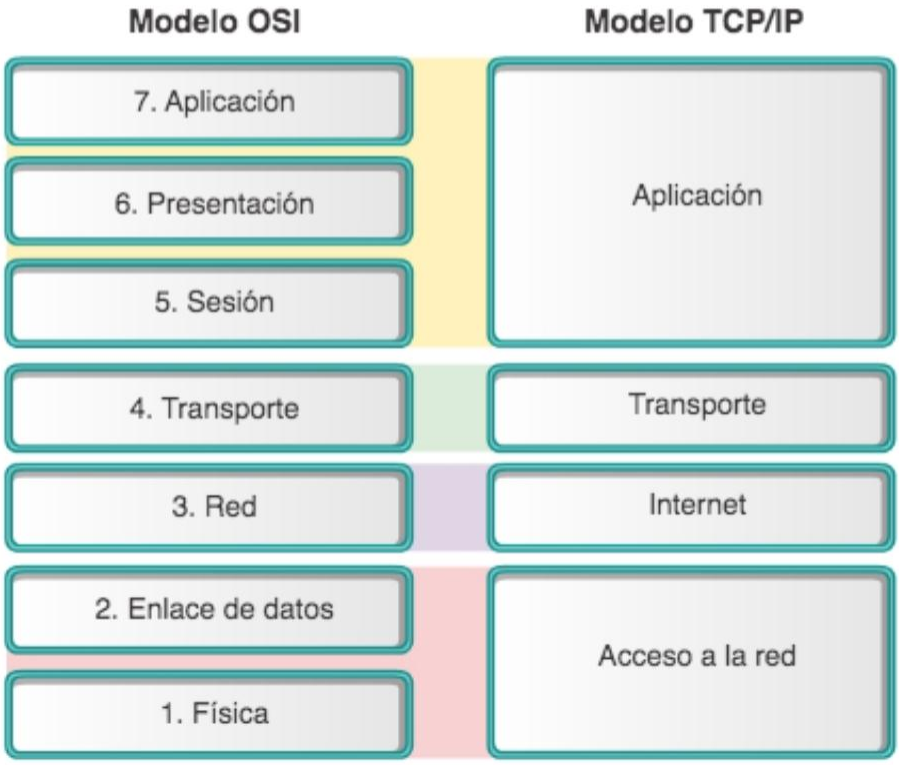
## 2.4 NIVELES DEL MODELO OSI




**E**l modelo OSI tiene siete capas. *Los principios que se aplicaron para llegar a las siete capas son los siguientes:*

1. Se debe crear una capa siempre que se necesite un nivel diferente de abstracción.
2. Cada capa debe realizar una función bien definida.
3. La función de cada capa se debe elegir pensando en la definición de protocolos estandarizada internacionalmente.
4. Los límites de las capas deben elegirse a modo de minimizar el flujo de información a través de las interfaces.
5. La cantidad de capas debe ser suficiente para no tener que agrupar funciones distintas en la misma capa y lo bastante pequeña para que la arquitectura no se vuelva inmanejable.

**Comparación del modelo OSI con el modelo TCP/IP**




Indudablemente, ambos modelos son de gran importancia al momento de estudiar las comunicaciones en redes, ya que definen la comunicación por medio de una arquitectura basada en capas (ver Figura 8). Sin embargo, existen algunas características entre uno y otro que los hacen diferentes, aunque el propósito para el que fueron creados sea el mismo.

En lo que se refiere al modelo OSI, se trata de un conjunto de siete capas, siendo la capa de aplicación la más cercana al usuario y la capa física la más alejada a él. En cada una de sus capas se ofrece un servicio que contribuye con una parte de la comunicación, dicho servicio es implementado a través de un protocolo y la manera de comunicarse con sus capas adyacentes es llevada a cabo mediante el establecimiento de una interfaz, es decir, la capa n solo puede comunicarse con las capas n-1 y n+1, siendo la capa física la que realmente conecta a ambas máquinas, ya que es a través de esta donde fluyen los mensajes en forma de bits.

## 2.5 MODELOS TCP/IP

Estos son basados en internet, y permite la trasmisión de datos entre las computadoras, como medio de comunicación y que también son guiados con todos los protocolos.

## 2.6 COMPARACIÓN

Se manejan los cuadros comparativos de los tipos de redes, como los nombres de la red y características, velocidad, así cada computador requiere de hardware para recibir y transmitir la información.

# UNIDAD III

# CAPAS DEL MODELO OSI Y TCP/IP

Es el protocolo de transporte que ofrece un servicio confiable de extremo a extremo en redes de datos tipo Internet. Desde su formulación a nuestros días, han surgido varias propuestas para poder adaptar este servicio a los más diversos requerimientos que la evolución de Internet a llevado consigo.

TCP se remota a los orígenes de Internet, derivada de ARPAnet a principios de los años 70. El primer protocolo conocido como TCP e IP. Poco tiempo después los requerimientos de nuevas aplicaciones mostraron la conveniencia de separar esas funciones en dos protocolos: uno de relevo de datagramas , IP y un protocolo confiable de extremo a extremo, TCP.

TCP se define como un protocolo de comunicación confiable, orientado a conexión entre procesos ejecutándose a equipos terminales (hosts) interconectados en un ambiente multiredes (Internet). Supone un servicio de transporte no confiable de las capas inferiores (notablemente IP), que le permite el envió de información en unidades de recepción de longitud variable llamadas segmentos. Cada segmento inicia con un encabezado que contiene información de control de TCP.

## 3.1 NIVELES DEL MODELO DE REFERENCIA OSI

**Nivel Físico**

La capa física tiene que ver con el envío de bits en un medio físico de transmisión y se asegura de que si de un lado del medio se envía un 1 del otro lado se reciba ese 1. También tiene que ver con la impedancia, resistencia y otras medidas eléctricas o electrónicas del medio y de qué forma tiene (tamaño, número de patas) en conector del medio y cuáles son los tiempos aprobados para enviar o recibir una señal. También se toma en cuenta si el medio permite la comunicación simplex, half duplex o full duplex.

## Nivel de Ligado

En esta capa se toman los bits que entrega la capa física y los agrupa en algunos cientos o miles de bits para formar marcos de bits. Se puede hacer en este nivel un chequeo de errores y si no los hay enviar un marco de acuse de recibo (acknowledge). Para detectar los límites de un marco se predefinen secuencias de bits de control. Si un marco se pierde o daña en el medio físico esta capa se encarga de retransmitirlo, aunque en ocasiones dicha operación provoca que un mismo frame se duplique en el destino, dado el caso es obligación de esta capa detectar tal anomalía y corregirla. También en esta capa se decide cómo accesar el medio físico.

## Nivel de red

La capa de red se encarga de controlar la operación de la subred (medios físicos y dispositivos de enrutado). Una tarea primordial es decidir cómo hacer que los paquetes lleguen a su destino dado un origen y un destino en un formato predefinido por un protocolo. Otra función importante en este nivel es la resolución de cuellos de botella. En estos casos se pueden tener varias rutas para dar salida a los paquetes y en base a algunos parámetros de eficiencia o disponibilidad se eligen rutas dinámicas de salida. Otra función que se puede obtener en esta capa es el registro o reporte del tipo y cantidad de paquetes que circulan por el enrutador para efectos de cobro o de obtención de estadísticas.

## Nivel de Transporte

La obligación en esta capa es la de tomar datos de la capa de sesión y asegurarse que dichos datos llegan a su destino. En ocasiones los datos que vienen de la capa de sesión exceden el tamaño máximo de transmisión (Maximum Transmission Unit MTU) de la interfaz de red, por lo cual es necesario partirlos y enviarlos en unidades más pequeñas, lo cual da origen a la fragmentación y ensamblado de paquetes cuyo control se realiza en esta capa.

Una vez que esta capa se encarga de procesar datos de la capa de sesión y servir de interfase con la de red, podemos afirmar que su función es la de separar a las capas superiores de los posibles cambios en el hardware de red.

Otra función en esta capa es la de multiplexar varias conexiones que tienen diferentes capacidades de transmisión para ofrecer una velocidad de transmisión adecuada a la capa de sesión. Por ejemplo, se puede decidir en un momento dado que una conexión es muy cara y que mejor se multiplexe sobre una conexión existente más barata para tener un ahorro. Estas decisiones son transparentes para la capa de sesión.

A partir de la capa de transporte (inclusive) las capas ofrecen servicios de interlocutor a interlocutor, esto es, que un programa de red en un nodo platica con otro programa similar en otro nodo de la red. En las capas inferiores esto no es posible ni requerido.

La última labor importante de la capa de transporte es ofrecer un mecanismo de nombrado que sirva para identificar y diferenciar las múltiples conexiones existentes, así como determinar en qué momento se inician y se terminan las conversaciones; es decir, en esta capa hay un mecanismo de control de flujo. Por ejemplo, si el usuario "operador" en el nodo "A" quiere iniciar una sesión de trabajo remoto (telnet) en un nodo "B", existirá una conexión que debe ser diferenciada de la conexión que el usuario "Luis" necesita para transferir un archivo (ftp) del nodo "B" al nodo "A".

Nivel de Sesión

Esta capa ofrece el servicio de establecer sesiones de trabajo entre nodos diferentes de una red. Permite el transporte de datos (soportado por la capa de transporte) y añade algunas facilidades para el establecimiento del flujo de datos.

Esta capa decide a quien se le hace caso para transmitir datos entre las múltiples conexiones, una manera de hacerlo es proveer de fichas a los participantes de una conexión, de manera que aquél que tenga la ficha es el que puede transmitir (lo cual es útil en un medio half duplex). Otro servicio de esta capa es la sincronización y el establecimiento de puntos de chequeo. Por ejemplo, si se hace necesario transferir un archivo muy grande entre dos nodos que tienen una alta probabilidad de sufrir una caída, es lógico pensar que una transmisión ordinaria nunca terminaría porque algún interlocutor se caerá y se perderá la conexión. La

solución es que se establezcan cada pocos minutos un punto de chequeo de manera que si la conexión se rompe más tarde se pueda reiniciar a partir del punto de chequeo, lo cual ahorrará tiempo y permitirá tarde o temprano la terminación de la transferencia.

### Nivel de Presentación

La capa de presentación nos provee de facilidades para que podamos transmitir datos con alguna sintaxis propia para nuestras aplicaciones o para nuestro nodo. Existen computadoras que interpretan sus bytes de una manera diferente que otras (Big Endian versus Little Endian). En esta capa es posible convertir los datos a un formato independiente de los nodos que intervienen en la transmisión.

### Nivel de Aplicación

En esta capa se encuentran aplicaciones de red que nos permiten explotar los recursos de otros nodos. Dicha explotación se hace, por ejemplo, a través de una emulación de una terminal que trabaja en un nodo remoto, interpretando una gran variedad de secuencias de caracteres de control que nos permiten desplegar en la terminal local los resultados, aún cuando éstos sean gráficos. Otra forma de explotación se da cuando transmitimos un archivo de una computadora que almacena sus archivos en un formato dado a una computadora de formato distinto. Es posible que el programa de transferencia realice las conversiones necesarias de manera que el archivo puede usarse inmediatamente bajo alguna aplicación.

## 3.2 TRANSMISIÓN DE DATOS EN EL MODELO OSI

Un envío de datos típico bajo el modelo de referencia OSI comienza con una aplicación P en un nodo cualquiera de la red. P genera los datos D que quiere enviar a su contraparte en otro nodo. Le pasa los datos D a la capa de aplicación .

La capa de aplicación toma los datos y los encapsula añadiendo un encabezado que contiene información de control o que puede estar vacío. El paquete completo resultante se lo pasa a la capa de presentación.

La capa de presentación lo recibe y no intenta siquiera decodificar o separar los componentes del paquete, sino que lo toma como datos y le añade un encabezado con información de control de esta capa y el paquete resultante se lo envía a la capa de sesión.

La capa de sesión recibe el paquete, que también son sólo datos para ella y le añade un encabezado de control. El resultado se lo envía a la capa de transporte.

La capa de transporte recibe todo el paquete como datos y le añade su propio encabezado de control creando otro paquete que envía a la capa de red, la cual se encargará de enrutarlo a su destino apropiado, entre otras actividades que realiza. Las capas de red, ligado de datos y física toman, respectivamente, el paquete que les envía la capa superior y añaden a éste un encabezado definido por el protocolo que corresponde a cada capa y pasan el resultada a la capa inferior. La capa física traducirá el último paquete a las señales apropiadas para que viajen por el medio físico hasta el nodo destino.

En el nodo destino, la capa física toma los paquetes y les quita el encabezado de la capa física, pasando el paquete resultante a la capa de ligado de datos. La capa de ligado lo recibe y le quita el encabezado de esta capa, pasando el resultado a la capa de red, quien lo toma y le quita el encabezado de red, pasando el paquete a la capa de transporte que elimina el encabezado de transporte y pasa el resultado a la capa de sesión, quien también le quita el encabezado respectivo y pasa el paquete a la capa de presentación, que a su vez le quita el encabezado de presentación y le pasa el paquete a la capa de aplicación que, finalmente, le quita el último encabezado y le entrega el paquete de datos reales a la aplicación en el nodo destino.

De manera virtual, se establecen conexiones directas entre las capas del mismo nombre de los dos diferentes nodos. Por ejemplo, el paquete que envía la capa de red es interpretado por la capa de red en el destino y no por otra capa. Para las capas inferiores de la de red, dicho paquete fue interpretado como datos, y para las capas superiores (transporte, sesión, presentación y aplicación) como un paquete compuesto de datos y encabezado.

Por otro lado, todas las capas, excepto la de aplicación, procesan los paquetes realizando operaciones que sólo sirven para verificar que el paquete de datos real esté íntegro o para que éste llegue a su destino, sin que los datos por sí mismos sufran algún cambio.

## 3.3 MODELO DE ARQUITECTURA DEL PROTOCOLO TCP/IP

El modelo OSI describe las comunicaciones de red ideales con una familia de protocolos. TCP/IP no se corresponde directamente con este modelo. TCP/IP combina varias capas OSI en una única capa, o no utiliza determinadas capas. La tabla siguiente muestra las capas de la implementación de Oracle Solaris de TCP/IP. La tabla enumera las capas desde la capa superior (aplicación) hasta la capa inferior (red física).

**Protocolos de las distintas capas de red**

| Ref. OSI Nº de capa | Equivalente de capa OSI | Capa TCP/IP | Ejemplos de protocolos TCP/IP |
|---|---|---|---|
| 5,6,7 | Aplicación, sesión, presentación | Aplicación | NFS, NIS, DNS, LDAP, telnet, ftp, rlogin, rsh, rcp, RIP, RDISC, SNMP y otros. |
| 4 | Transporte | Transporte | TCP, UDP, SCTP |
| 3 | Red | Internet | IPv4, IPv6, ARP, ICMP |
| 2 | Vínculo de datos | Vínculo de datos | PPP, IEEE 802.2 |
| 1 | Física | Red física | Ethernet (IEEE 802.3), Token Ring, RS-232, FDDI y otros. |

## 3.4 CAPA DE INTERNET/RED

La capa de Internet, también conocida como capa de red o capa IP, acepta y transfiere paquetes para la red. Esta capa incluye el potente Protocolo de Internet (IP), el protocolo de resolución de direcciones (ARP) y el protocolo de mensajes de control de Internet (ICMP).
Protocolo IP
El protocolo IP y sus protocolos de enrutamiento asociados son posiblemente la parte más significativa del conjunto TCP/IP. El protocolo IP se encarga de:

Direcciones IP: Las convenciones de direcciones IP forman parte del protocolo IP. Cómo diseñar un esquema de direcciones IPv4 introduce las direcciones IPv4 y Descripción general de las direcciones IPv6 las direcciones IPv6.
Comunicaciones de host a host: El protocolo IP determina la ruta que debe utilizar un paquete, basándose en la dirección IP del sistema receptor.

Formato de paquetes: el protocolo IP agrupa paquetes en unidades conocidas como datagramas. Puede ver una descripción completa de los datagramas en Capa de Internet: preparación de los paquetes para la entrega.

Fragmentación: Si un paquete es demasiado grande para su transmisión a través del medio de red, el protocolo IP del sistema de envío divide el paquete en fragmentos de menor tamaño. A continuación, el protocolo IP del sistema receptor reconstruye los fragmentos y crea el paquete original.

Para evitar confusiones con el uso del Protocolo de Internet, se utiliza una de las convenciones siguientes:

Cuando se utiliza el término "IP" en una descripción, ésta se aplica tanto a IPv4 como a IPv6.
Cuando se utiliza el término "IPv4" en una descripción, ésta sólo se aplica a IPv4.
Cuando se utiliza el término "IPv6" en una descripción, ésta sólo se aplica a IPv6.

**Enrutamiento y sus características.**

Se conoce con el nombre de enrutamiento (routing) el proceso que permite que los paquetes IP enviados por el host origen lleguen al host destino de forma adecuada.

En su viaje entre ambos host los paquetes han de atravesar un número indefinidos de host o dispositivos de red intermedios, debiendo existir algún mecanismo capaz de direccionar los paquetes correctamente de uno a otro hasta alcanzar el destino final. Este mecanismo de ruteo es responsabilidad del protocolo IP, y lo hace de tal forma que los protocolos de las capas superiores, como TCP y UDP, no tienen constancia alguna del mismo, limitándose a preocuparse de sus respectivas tareas.

## 3.5 PROTOCOLO UDP

UDP o Protocolo de Datagrama de Usuario (User Datagram Protocol) es un protocolo que permite la transmisión de datos sin conexión previa; de esta manera, es posible enviar información de una forma muy rápida, sin necesidad de confirmar la conexión, y esperar la respuesta de que los paquetes fueron recibidos correctamente.

El Protocolo UDP pertenece a la familia de protocolos de Internet de la Capa 4 de Transporte del Modelo de Referencia OSI. Proporciona una sencilla interfaz entre la Capa de Red y las superiores (Sesión, Presentación y Aplicación), no otorga garantías para la entrega de sus mensajes, y no retiene el estado de los paquetes que han sido enviados a la red.

UDP permite el envío de datagramas a través de la red sin que se haya establecido previamente una conexión, ya que el propio datagrama incorpora suficiente información de direccionamiento en su cabecera. Tampoco tiene confirmación ni control de flujo, por lo que los paquetes pueden adelantarse unos a otros, y tampoco se sabe si han llegado todos correctamente, ya que no hay confirmación de entrega o recepción.

El Protocolo UDP proporciona muy pocos servicios de recuperación de errores, ofreciendo en su lugar una manera directa y rápida de enviar y recibir datagramas a través de una red; es empleado fundamentalmente para la comunicación entre sistemas, en los que la velocidad es más importante que la fiabilidad en la transmisión de la información.

Se utiliza UDP para enviar paquetes de datos desde un emisor a un receptor, sin importar que este último los reciba todos completamente. Cada paquete es enviado directa e individualmente sin establecerse ni reconocerse un canal de datos fiable.

En pos de la velocidad de envío, no existe un orden inherente en la transmisión de los paquetes de datos, pues todos se envían a través de la red de forma independiente entre sí. De igual modo, no es posible solicitar los paquetes de datos que faltan una vez que se pierden en tránsito.

En un flujo continuo muy rápido de información, como la transmisión en directo de televisión por Internet, por ejemplo, se utiliza el protocolo UDP, pues la pérdida de algunos paquetes en tránsito, aunque causa cierta distorsión de imagen o audio, no afecta considerablemente la reproducción del video.

Características

Para comprender a fondo cómo funciona la transmisión de paquetes del Protocolo UDP, resulta útil analizar detenidamente cuáles son sus propiedades fundamentales:

Funciona sin conexión: el protocolo UDP se caracteriza porque permite el envío de paquetes a través de la red sin que se haya establecido previamente una conexión entre el emisor y el receptor. Los datagramas respectivos se envían a la dirección IP especificando el puerto de destino, sin que sea necesario una confirmación de llegada como respuesta.

Utiliza puertos: para permitir que los datagramas se transfieran a las aplicaciones correctas, elegidas en el dispositivo de destino. Los puertos quedan definidos mediante un número conforme a un rango de valores válidos.

Permite una comunicación sin retardos: es el adecuado para una transmisión de datos rápida debido a que no hay que llevar a cabo una configuración de la conexión, lo que resulta también del hecho de que la pérdida de un paquete individual afecta exclusivamente a la calidad de la transmisión, y no la transmisión en sí.

No ofrece garantía de seguridad de los datos: la ausencia de acuse de recibo mutuo entre el emisor y el receptor garantiza que la velocidad de transmisión sea excelente; no obstante, no puede asegurar la integridad de los datagramas; tampoco puede garantizar el orden de los paquetes enviados; por ello, los servicios que utilizan UDP deben aplicar sus propias medidas de corrección y protección.

El Protocolo UDP no proporciona una entrega de datos fiable, sin embargo, existen aplicaciones, por ejemplo, interesadas en transmitir información en modo multicast o broadcast (a un grupo o a todos los usuarios de la red) sin esperar una respuesta, de manera que UDP es ideal para esta función.

## 3.6 DATAGRAMA UDP

El datagrama UDP consta de una cabecera de 64 bits (8 bytes), y un cuerpo para encapsular los datos de longitud variable.

La cabecera consta de 4 campos de 16 bits cada uno, y de los cuales 2 son opcionales:

Puerto de origen: es el número de puerto relacionado con la aplicación del emisor del segmento UDP. Este campo representa una dirección de respuesta para el destinatario, por lo tanto, es opcional, y si no se especifica, se completa con 0, y el destinatario no podrá responder (lo cual no es estrictamente necesario, en particular para mensajes unidireccionales).

Puerto de destino: este campo contiene el puerto correspondiente a la aplicación del equipo receptor al que se envía.

Longitud: indica el tamaño completo en byte del datagrama UDP, incluyendo la cabecera. La longitud mínima de un datagrama UDP es de 8 bytes (64 bits: 16 por cada campo de la cabecera y 0 en el cuerpo), y la máxima de 65.535 bytes.
Suma de comprobación: es una suma de comprobación realizada de manera tal que permita controlar la integridad del segmento, protegiendo tanto la cabecera como los datos; es opcional, aunque en la práctica se utiliza.
El cuerpo de datagrama UDP se emplea para el transporte de los datos que se intercambian entre las aplicaciones.

**Aplicaciones sobre UDP**

Existen fundamentalmente tres tipos de aplicaciones que son muy adecuadas para emplear el protocolo UDP:

Aplicaciones que pueden tolerar cierta pérdida de datos, pero requieren retrasos cortos o que no haya retrasos.

Aplicaciones con transacciones de solicitud y respuesta simples.

Comunicaciones unidireccionales donde no se requiere confiabilidad o donde la aplicación la pueda administrar.

Muchas aplicaciones de video y multimedia, como VoIP (Voice over IP o Voz sobre IP) e IPTV (IP Television o Televisión por IP) utilizan UDP, ya que pueden tolerar cierta pérdida de datos con un efecto mínimo o imperceptible. Los mecanismos de confiabilidad de otros protocolos, presentan cierto grado de demora que se puede percibir en la calidad de sonido o video que se recibe.

Otro tipo de aplicaciones adecuadas para UDP son las que utilizan transacciones de solicitud y respuesta simples, lo que significa que envían una solicitud, y puede o no recibir respuesta; incluso, en caso negativo, pueden volver a intentar la solicitud. Algunas de ellas son: DNS

(Domain Name System o Sistema de Nombres de Dominio), DHCP (Dynamic Host Configuration Protocol o Protocolo de Configuración Dinámica de Host), y SNMP (Simple Network Management Protocol o Protocolo Simple de Gesión de Red), entre otras

Algunas aplicaciones, además, se ocupan de la confiabilidad por sí mismas, por lo que no necesitan de mecanismos de seguridad adicionales de otros protocolos, y emplean por tanto UDP. TFTP (Trivial File Transfer Protocol o Protocolo de Transferencia Trivial de Archivos) es un ejemplo de este tipo de aplicaciones, pues presenta mecanismos propios para el control del flujo, la detección de errores, los acuses de recibo y la recuperación de errores. Este protocolo se utiliza principalmente para actualizar el firmware y el software de los dispositivos.

En todos los casos anteriores, la baja sobrecarga de transporte del Protocolo UDP, lo hacen deseable para ser empleado por dichas aplicaciones.

## 3.7 UDP vs TCP

En una referencia al Modelo OSI, tanto el Protocolo de Control de Transmisión (TCP) como el Protocolo de Datagrama de Usuario (UDP), pertenecen a la Capa 4 de Transporte; ambos cumplen funciones diferentes, y trabajan mejor para tareas específicas y en algunos casos combinadas, para explotar óptimamente los puntos fuertes de cada uno.

**Algunas de las principales diferencias entre TCP y UDP pueden resumirse como**:

El protocolo TCP está orientado a la conexión, lo que significa que verifica la correcta transmisión de datos entre el emisor y el receptor, mientras que UDP es un protocolo sin previa conexión, que se traduce en el hecho de no chequear que los datos realmente lleguen a su destino correctamente.

TCP es altamente confiable para transferir datos, ya que analiza el acuse de recibo de la información enviada, y reenvía los paquetes perdidos. UDP no gestiona la pérdida de

paquetes, por tanto, no solicita su retransmisión, por lo que se considera en este sentido un protocolo poco fiable.

TCP es más lento para el envío de información que UDP, ya que TCP establece la conexión antes de transmitir los datos y garantiza la entrega adecuada de los paquetes; UDP por su parte, simplemente envía los datos de manera directa y rápida.

El tamaño de cabecera de los paquetes de datos TCP es de 20 bytes, mientras que el UDP es de solo 8 bytes; lo que responde a la necesidad del primero de incluir más información en los paquetes, para poder comprobar y subsanar posibles errores después de la transmisión.

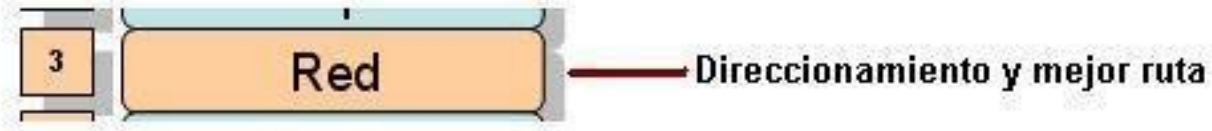
Tanto TCP como UDP pueden comprobar si hay errores, pero sólo TCP puede corregir el error ya que tiene control de congestión y de flujo.

En resumen, tanto TCP como UDP tienen ventajas y desventajas: UDP es más rápido y simple, por tanto, generalmente se utiliza para el envío de datos que no permiten retrasos; mientras TCP por otro lado, es robusto y fiable, garantizando la entrega de paquetes y la seguridad de la comunicación.

En función de las necesidades de las aplicaciones, se recomienda el uso de uno u otro, incluso combinados, para explotar al máximo sus potencialidades en la transmisión de datos.

## 3.8 CAPA DE RED

La Capa de red o Capa 3 de OSI provee servicios para intercambiar secciones de datos individuales a través de la red entre dispositivos finales identificados. Para realizar este transporte de extremo a extremo la Capa 3 utiliza cuatro procesos básicos:



- direccionamiento
- encapsulamiento
- enrutamiento
- desencapsulamiento

**Direccionamiento**

Primero, la Capa de red debe proveer un mecanismo para direccionar estos dispositivos finales. Si las secciones individuales de datos deben dirigirse a un dispositivo final, este dispositivo debe tener una dirección única. En una red IPv4, cuando se agrega esta dirección a un dispositivo, al dispositivo se lo denomina host.

**Encapsulación**

Segundo, la capa de Red debe proveer encapsulación. Los dispositivos no deben ser identificados sólo con una dirección; las secciones individuales, las PDU de la capa de Red, deben, además, contener estas direcciones. Durante el proceso de encapsulación, la Capa 3 recibe la PDU de la Capa 4 y agrega un encabezado o etiqueta de Capa 3 para crear la PDU de la Capa 3. Cuando nos referimos a la capa de Red, denominamos paquete a esta PDU. Cuando se crea un paquete, el encabezado debe contener, entre otra información, la dirección del host hacia el cual se lo está enviando. A esta dirección se la conoce como dirección de destino. El encabezado de la Capa 3 también contiene la dirección del host de origen. A esta dirección se la llama dirección de origen. Después de que la Capa de red completa el proceso de encapsulación, el paquete es enviado a la capa de enlace de datos que ha de prepararse para el transporte a través de los medios.

**Enrutamiento**

Luego, la capa de red debe proveer los servicios para dirigir estos paquetes a su host destino. Los host de origen y destino no siempre están conectados a la misma red. En realidad, el paquete podría recorrer muchas redes diferentes. A lo largo de la ruta, cada paquete debe ser guiado a través de la red para que llegue a su destino final. Los dispositivos intermediarios

que conectan las redes son los routers. La función del router es seleccionar las rutas y dirigir paquetes hacia su destino. A este proceso se lo conoce como enrutamiento.

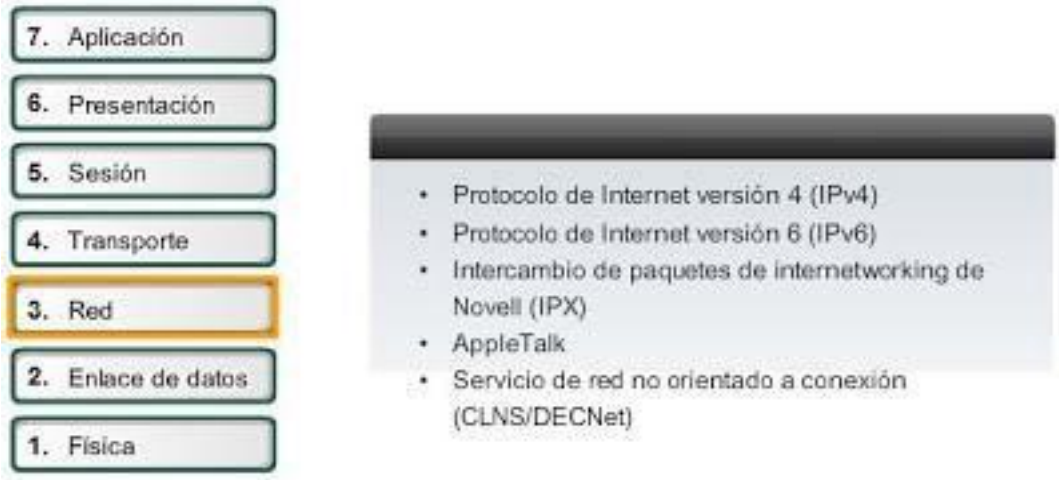
### Desencapsulamiento

Finalmente, el paquete llega al host destino y es procesado en la Capa 3. El host examina la dirección de destino para verificar que el paquete fue direccionado a ese dispositivo. Si la dirección es correcta, el paquete es desencapsulado por la capa de Red y la PDU de la Capa 4 contenida en el paquete pasa hasta el servicio adecuado en la capa de Transporte.

### Protocolos de la capa de red

Los protocolos implementados en la capa de Red que llevan datos del usuario son:

- Versión 4 del Protocolo de Internet (IPv4)




- Versión 6 del Protocolo de Internet (IPv6)
- Intetercambio Novell de paquetes de internetwork (IPX)
- AppleTalk
- Servicio de red sin conexión (CLNS/DECNet)

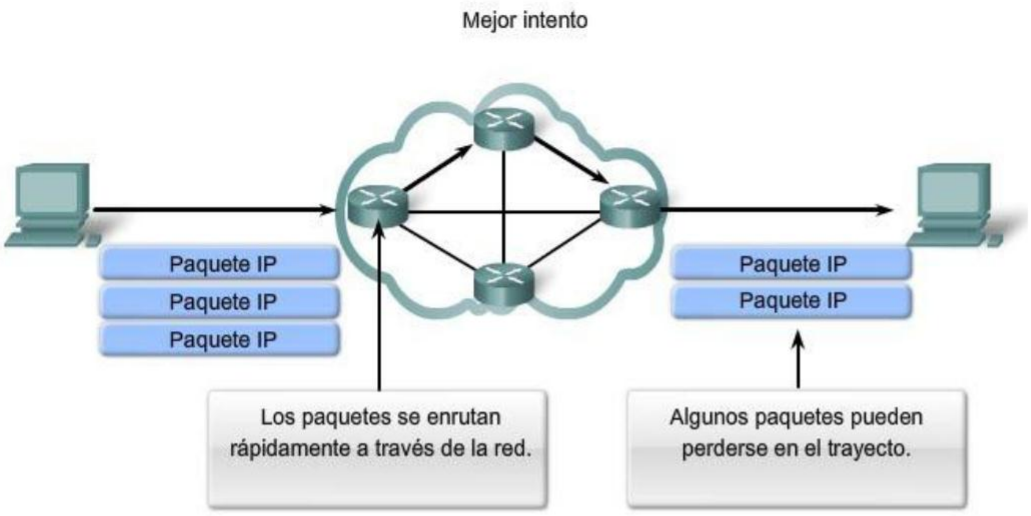
## 3.9 IPV4

La versión 4 de IP (IPv4) es la versión de IP más ampliamente utilizada. Es el único protocolo de Capa 3 que se utiliza para llevar datos de usuario a través de Internet y es el tema de CCNA.

El Protocolo de Internet fue diseñado como un protocolo con bajo costo. Provee sólo las funciones necesarias para enviar un paquete desde un origen a un destino a través de un sistema interconectado de redes. El protocolo no fue diseñado para rastrear ni administrar el flujo de paquetes. Estas funciones son realizadas por otros protocolos en otras capas.

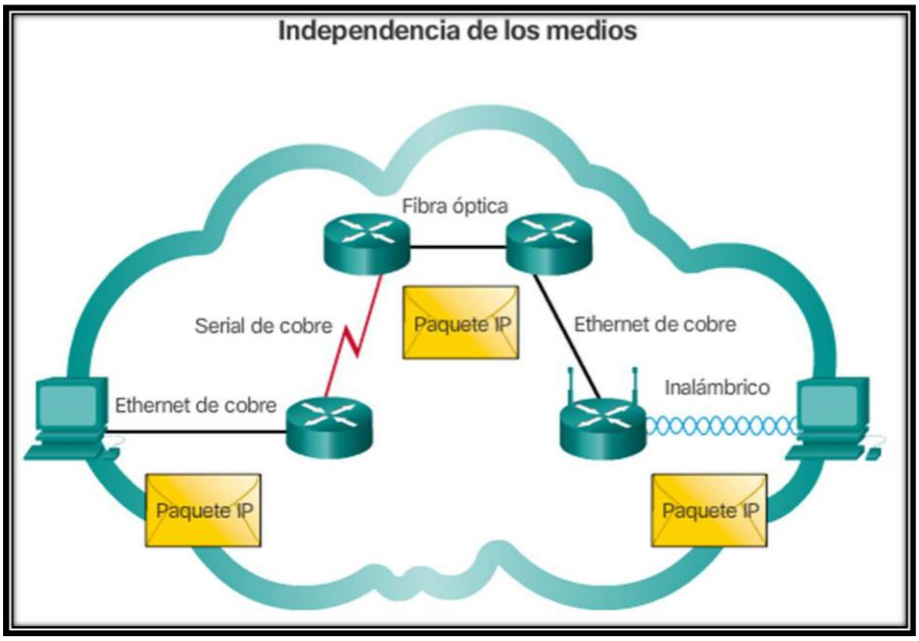
Características básicas de IPv4:

- Sin conexión: No establece conexión antes de enviar los paquetes de datos.
- Máximo esfuerzo (no confiable): No se usan encabezados para garantizar la entrega de paquetes.
- Medios independientes: Operan independientemente del medio que lleva los datos.




Al ser un protocolo no confiable de capa de red, IP no garantiza la recepción de todos los paquetes enviados.

Otros protocolos administran el proceso de seguimiento de paquetes y garantizan su entrega.




## IPv6

El Protocolo de Internet versión 6, en inglés: Internet Protocol version 6 (IPv6), es una versión del Internet Protocol (IP), definida en el RFC 2460 y diseñada para reemplazar a Internet Protocol version 4 (IPv4) RFC 791, que a 2016 se está implementado en la gran mayoría de dispositivos que acceden a Internet.

IPv6 es una extensión conservadora de IPv4. La mayoría de los protocolos de transporte -y aplicación- necesitan pocos o ningún cambio para operar sobre IPv6; las excepciones son los protocolos de aplicación que integran direcciones de capa de red, como FTP o NTP. IPv6 especifica un nuevo formato de paquete, diseñado para minimizar el procesamiento del encabezado de paquetes. Debido a que las cabeceras de los paquetes IPv4 e IPv6 son significativamente distintas, los dos protocolos no son interoperables. Algunos de los cambios de IPv4 a IPv6 más relevantes son:

- Capacidad extendida de direccionamiento
- Autoconfiguración de direcciones libres de estado (SLAAC)
- Multicast
- Seguridad de Nivel de Red obligatoria
- Procesamiento simplificado en los routers
- Movilidad
- Soporte mejorado para las extensiones y opciones
- Jumbogramas

**IPX**

IPX. Son las siglas en inglés de Internetwork Packet Exchange (Intercambio de Paquetes Interred). Es un protocolo de la capa de red de Netware responsable de transferir datos entre el servidor y los programas de las estaciones de trabajo mediante datagramas.

IPX es un antiguo protocolo de red de Novell perteneciente al sistema operativo NetWare. Se utiliza para transmitir datos a través de la red, incluyendo en cada paquete la dirección de destino. Es un protocolo de datagramas rápido orientado a comunicaciones sin conexión.

Características:

- IPX es un protocolo de la Capa de red (nivel 3 del modelo OSI).

- Está orientado a paquetes y a comunicaciones sin conexión (no requiere que se establezca una conexión antes de que los paquetes se envíen a su destino).
- Es utilizado como mensajero del protocolo SPX, ya que por sí solo carece de fiabilidad durante el transporte de paquetes.
- La cabecera de los paquetes de IPX se compone de 30 bytes, y los datos que junto con la cabecera no pueden sobrepasar los 1518 bytes.
- Sistema de direccionamiento IPX


Se utilizan tres componentes básicos para identificar un proceso en la red:

- Dirección de red, la cual identifica la red a la que pertenece.
- Número de nodo que indica el dispositivo conectado a la red.
- Número de socket que indica el proceso en el nodo.

## Appletalk

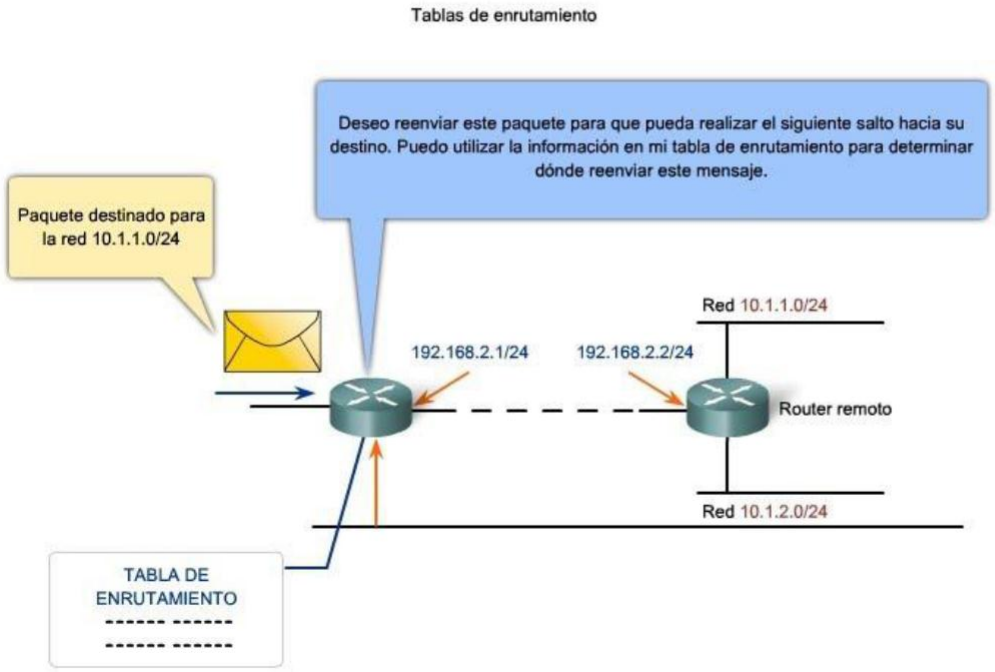
Appletalk es un conjunto de protocolos desarrollados por Apple Inc. para la interconexión de redes locales. Fue incluido en un Macintosh Apple en 1984 y actualmente está en desuso en los Macintosh en favor de las redes TCP/IP.
el protocolo utilizado en la capa numero 3 es el DDP (Datagram Delivery Protocol) que realiza el transporte de datos de bajo nivel.

**CLNS**

CLNS (Servicio No Orientado a Conexión), en telecomunicaciones, es un servicio que establece la comunicación entre entidades sin necesidad de establecer una conexión entre ellas. Cuando una entidad tiene información para transmitir, sencillamente la envía, (tramas, paquetes, bloques, etc.).
Funcionamiento
El proveedor trata cada objeto de información de forma independiente y autónoma, incluso aunque se trate de un conjunto de objetos pertenecientes al mismo mensaje. El usuario confía simplemente en que cada objeto ha de llegar a su destino más pronto o más tarde. Los servicios orientado y no orientado a conexión, se suelen asimilar con los servicios telefónico y postal respectivamente. El sistema telefónico es un ejemplo de servicio orientado a conexión, mientras que el sistema postal es un servicio no orientado a conexión. Esta analogía es perfectamente aplicable a la funcionalidad y a la lógica de los servicios CONS y CLNS.

Cuando un host debe enviar datos a otro, lo primero que hace es comprobar si la dirección IP de éste se encuentra en su tabla ARP, en cuyo caso los datagramas le son enviados directamente mediante la dirección de su tarjeta de red, conocida como dirección física.

En caso de que no conozca la misma, envía un mensaje de petición ARP, que será respondido por el host destino enviando su dirección física, con la que ya tiene los datos suficientes para la transmisión de las tramas. Este proceso recibe el nombre de routing directo.




Si el host B de la red A deséa enviar un paquete al host H, lo primero que hará será comprobar si el host de destino aparece en su tabla de resoluciones ARP, y si no es así, realiza la correspondiente petición ARP usando broadcast. Como H no puede responder a la misma, al estar en otra red, B decide enviar los paquetes al router para que éste se encargue de su direccionamiento. Los paquetes que le pasa contienen la dirección IP de H y la dirección física del router.

Los routers poséen unas tablas de enrutamiento en las que almacenan información sobre el mejor camino que pueden seguir los paquetes para llegar a su destino. Cuando le llegan los paquetes, el router debe extraer de ellos la dirección de la red a la que pertenece H, para saber a cuál de las redes que una debe mandar los paquetes. Para ello, coge la dirección IP de destino y realiza con ella y las máscaras de red de cada una de las redes a las que pertenece una operación AND lógica, con lo que obtendrá la dirección de la red destino. Para realizar la operación AND pasa las direcciones IP a formato binario

Los Routers aprenden acerca de la topología de la red en base a:

- Rutas estáticas
- Protocolos de enrutamiento.

**Rutas Estáticas:** Se administra en forma manual por el administrador de la red, ya que este es el encargado de actualizar las rutas y las modificaciones se hacen de forma manual.

- Permiten la configuración manual de las tablas de enrutamiento.
- Las tablas no podrán ser modificadas en forma dinámica
- Falta de flexibilidad frente a fallas de los enlaces
- No son necesarios las cargas y procesos asociados a un protocolo de descubrimiento de rutas.
- Es fácil establecer barreras de seguridad bajo este modelo.

**Enrutamiento Dinámico:** El administrador configura el routing de este manera el protocolo administra los cambios mediante el envió periódico de información de enrutaminto.

- Se basa en la comunicación, a través de broadcasts, entre los routers.
- Para descubrir las mejores rutas los routers emplean el concepto de métrica.
- No es necesario mantener manualmente las tablas de rutas.

El direccionamiento IP

Los equipos y redes que funcionan mediante el protocolo TCP/IP (Protocolo de Control de Transmisión / Protocolo de Internet). Este protocolo necesita para su funcionamiento que los equipos que funcionan con él tengan dos parámetros configurados en su interfaz de red, estos son la dirección IP y la máscara de subred.

## Dirección IP

En primer lugar, tenemos la dirección IP, que prácticamente todos conoceremos. Es una dirección lógica de 4 bytes o 32 bits cada uno de ellos separados por un punto, con la que se identifica unívocamente a un equipo o host en una red.

En la actualidad los equipos cuentan con dos tipos de direcciones IP, en primer lugar, está la dirección IPv4 que efectivamente tiene una longitud de 4 bytes (0 – 255) y que podríamos representarla de la siguiente forma:

| | |
|---|---|
| Notación decimal (la más conocida) | 192.168.3.120 |
| Notación binaria | 11000000.10101000.00000011.01111000 |
| Notación hexadecimal | C0 A8 03 78 |

Y la dirección IPv6, que está diseñada para el caso en que el direccionamiento IP tradicional se quede corto. En este caso tendremos una dirección lógica de 128 bits, por lo que abarca un rango mucho más amplio que la dirección IPv6. Esta la veremos escrita casi siempre en formato hexadecimal:

```
2010:DB92:AC32:FA10:00AA:1254:A03D:CC49
```

Estamos ante una cadena de hasta 8 términos separados mediante los dos puntos en donde cada uno puede representar 128 bits.

En nuestro caso, en el 100% de ocasiones, utilizaremos para el direccionamiento IP el método tradicional de la dirección IPv4, así que este será el que veamos.

## 3.10 LOS CAMPOS DE RED Y HOST Y TIPO DE DIRECCIÓN IP

Una dirección IP se puede dividir en dos partes llamadas red y host. En función de estos dos campos tendremos estos tipos de direcciones IP:

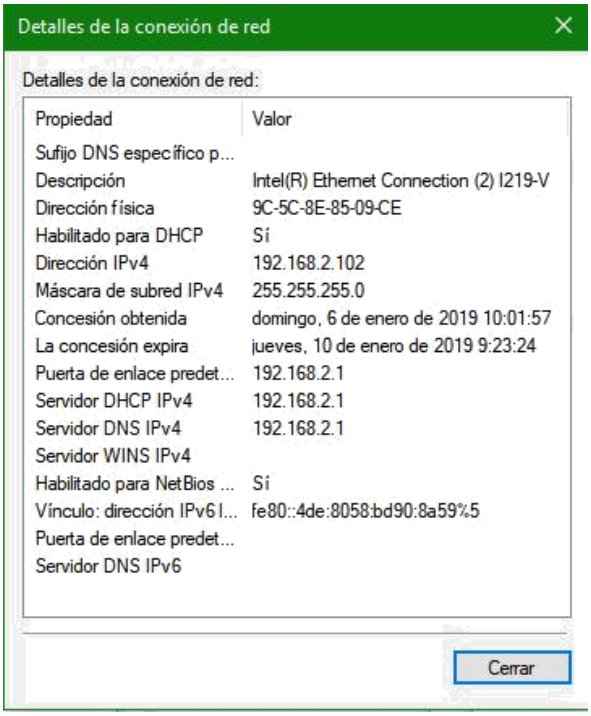
Clase A: solamente utilizamos el primer byte para definir la red en donde nos encontramos. Los tres bytes siguientes estarán destinados a identificar al host dentro de esta red. El rango de direcciones va desde la 0.0.0.0 hasta la 127.255.255.255. La clase A se utiliza para redes muy grandes ya que tendremos direccionamiento hasta para 16 millones de equipos.

Clase B: en este caso estaríamos utilizando los dos primeros bytes de la dirección para definir la red y los otros dos para definir el host. Este rango va desde 128.0.0.0 hasta la 191.255.255.255. también está destinado a redes de extensor tamaño.

Clase C: en este caso utilizamos los tres primeros bytes para direccionar redes y el último byte para definir el host. De esta forma tendremos el muy conocido rango de 0.0.0 hasta 223.255.255.255.

Clase D: el rango de IP de clase D no es de utilización común para usuarios normales, ya que está destinado a su uso experimental y grupos de máquinas concretos. Este rango va desde 224.0.0.0 hasta 239.255.255.255.

Clase E: finalmente tenemos la clase E, la cual tampoco se utiliza en equipos de uso normal.
En este caso tendremos un rango que comienza en el byte 223.0.0.0 hasta el resto.




## Máscara de subred

Una vez conocidas las propiedades de direccionamiento IP para los hosts dentro de una red, pasamos a ver otro parámetro no menos importante, que es la máscara de subred.

Para cada clase de IP se puede contar con un número de subredes determinado. Una subred es una red física independiente que comparte la misma dirección IP con otras redes físicas, es decir, ahora estamos identificando a la red principal en donde se conectan los hosts.

Precisamente la función de la máscara de subred es lograr que equipos que comparten el mismo identificar de red y que están situados en redes físicas distintas se puedan comunicar. Será nuestro router o servidor el que haga la correspondencia entre la información de la máscara de subred y la dirección IP de los hosts.

Existen tres tipos de máscaras de subred, para cada una de las clases utilizadas:

| | |
|---|---|
| A | 255.0.0.0 |
| B | 255.255.0.0 |
| C | 255.255.255.0 |

## Cómo obtener la dirección de red y host

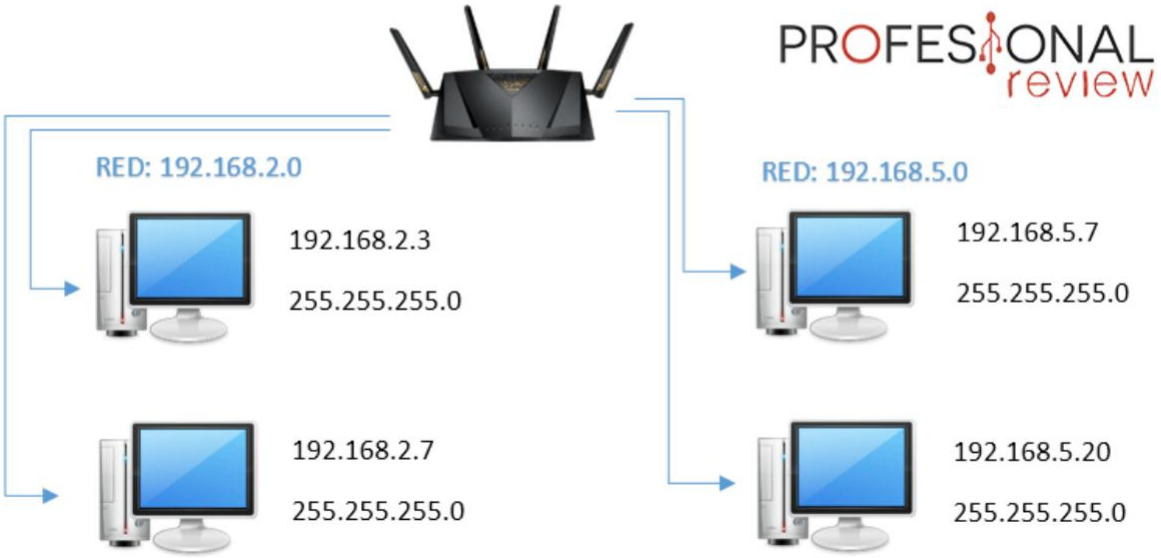
Ahora la cuestión es saber cómo un router puede identificar la red a la que pertenece un host para diferenciarlo de otra red distinta. El procedimiento es bien sencillo si sabemos la dirección IP y la máscara de subred, lo que tendremos que hacer una operación AND en binario. Por ejemplo:

Dirección IP de host: 181.20.6.19 (10110101.010100.000110.010011) Máscara de subred: 255.255.0.0 (111111.111111.000000.000000)

Operación AND binaria: (solamente será 1 si ambos caracteres son 1)

Resultado: 181.20.0.0 (10110101.010100.000000.000000)

Entonces, está será la red a la que pertenece el host con dirección 181.20.6.19. Fácil.




## Notación abreviada dirección-mascara

Seguramente hayas visto en bastantes ocasiones la notación de 192.168.1.1/24 o 180.10.1.1/16. Vamos a ver qué significa esto rápidamente.

Cuando vemos esta notación lo que estamos leyendo es la dirección IP de un host, en este caso podría ser la dirección IP de un router y los bits asignados a la identificación de la red. Entonces:

Si tenemos 192.168.1.1/24, significa que los 24 primeros bits (en binario) están destinados a la red, por lo que la máscara de subred sería 255.255.255.0, y la red a la que pertenece sería 192.168.1.0.

Si tenemos 180.10.1.1/16, significará que los primeros 16 bits están destinados a la red, entonces sería 255.25.0.0, y la red a la que pertenece sería 180.10.0.0.

## Manejo de subredes

Cuando definimos una red se debe de tomar en cuenta el número de nodos que esta va a tener ya que es indispensable para tener una idea concreta de qué tipo de red necesitamos.
La red se divide por su funcionalidad y tamaño

Todos los dispositivos necesitan una dirección IP para la comunicación con otros dispositivos, como por ejemplo los dispositivos finales, como son el equipo de usuario, equipo de administradores, servidores e impresoras, teléfono IP y cámaras IP.

Entre los dispositivos de red que requieren una dirección IP se incluyen:

- Interfaces LAN del Router
- Interfaces (serial) WAN del Router

Entre los dispositivos de red que requieren una dirección IP esta el Switch

Primero se establece el total de Hosts, después se considera las direcciones disponibles y donde encajan en la dirección de red determinada.

Las redes se dividen por su finalidad y por su tamaño.
Sustraemos las direcciones de red y de broadcast.
Las direcciones más bajas se le van a asignar a la red y la última no se le es asignada a nadie ya que es la del broadcast
Todos los elementos de la red tienen un nombre de red en este caso una dirección IP.
Cada grupo de nodos de una red que se comunican de una manera privada tiene su propio dominio de colision

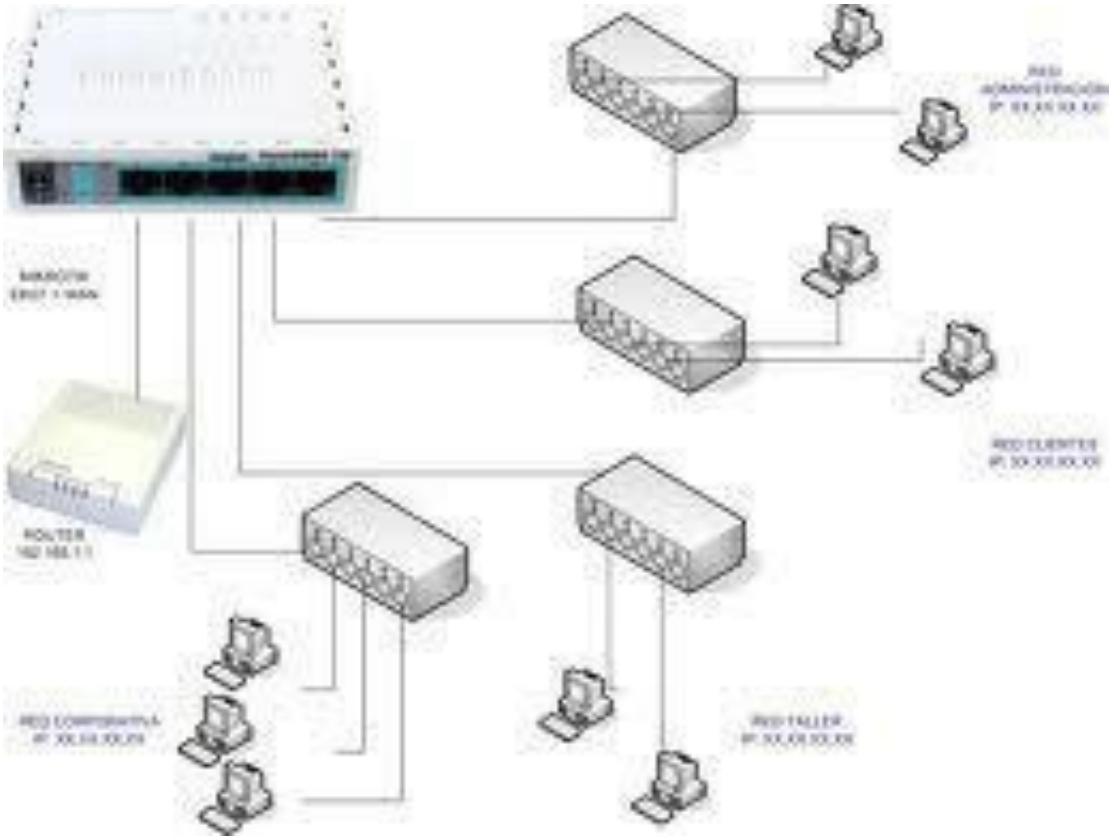
## Razones para dividir una red en subredes

El propósito de tener una subred es realizar las tareas de una manera más rápida, entendible y sencillas.

**Administrar** El tráfico de brodcasts: tienen su propio dominio de brodcasts, (un mensaje inunda toda la red y esto hace que se comunique o entienda el mensaje a donde se envió). No todos los hosts del sistema reciben todos los broadcasts

Diferentes requisitos de red: se agrupan los requisitos para asignarles una función en específico porque así resulta más sencillo administrarlo.

**Seguridad**: diferentes niveles de acceso



## Numero de subredes

Segmento físico: de la red requiere una interfaz de Router que funciones como Gateway para tal subred.

Además, cada conexión entre los routers constituye una red independiente

Por cada subred se necesita un Gateway (compuerta lógica de salida y entrada, se le hacen las preguntas y manda respuestas, te dirige a la dirección que preguntas) dependiendo el tipo de enlace que realices si es directo indica a que dirección tiene que ir dirigido el mensaje si es indirecto pregunta a otro Gateway hasta llegar al destino y por fin poder entablar la comunicación:

- La red se comunica de Gateway a Gateway.
- Entre router y router no hay Gateway.
- Gateway siempre se le asigna una dirección IP
- Ruter a Ruterà comunicación WAN
- Ruter a hubà Comunicación LAN

**vlsm y cidr**

VLSM Variable Length Subnet Masking. VLSM es una técnica introducida en 1987 por la IETF en laRFC 1009 con el objetivo de brindar mayor flexibilidad a laaplicación de subredes.El subneteo con VLSM (Variable Length Subnet Mask), máscara variable ó máscara de subred de longitud variable,es uno de los métodos que se implementó para evitar elagotamiento de direcciones IPv4 permitiendo un mejoraprovechamiento y optimización del uso de direcciones.Es el resultado del proceso por el cual se divide una red osubred en subredes más pequeñas cuyas máscaras sondiferentes según se adaptan a las necesidades de hosts por subred.

Características VLSM.

Hay varios factores a tener en cuenta a la hora de subnetear y trabajar con VLSM. El uso de VLSM solo es aplicable con los protocolos de enrutamiento sin clase RIPv2, OSPF, EIGRP, BGP4 e IS-IS.

Al igual que en el subneteo, la cantidad de subredes y hosts está supeditada a la dirección IP de red o subred que nos otorguen.

Implementación VLSM

Ventajas de la VLSM:

- Permite el uso eficaz del espacio de direccionamiento
- Permite el uso de varias longitudes de la máscara de subred
- Divide un bloque de direcciones en bloques más pequeños
- Permite la sumarización de ruta
- Proporciona mayor flexibilidad en el diseño de red
- Soporta redes empresariales jerárquicas

**CONCLUSIONES**: El VLSM es una técnica muy importante que nos facilita administrar nuestras redes de una manera mas eficiente,ya que a la hora de dividirlas se aprovecha el máximo de estas, así solo pocas direcciones se desperdician.

CIDR Enrutamiento Inter-Dominios sin Clases Se introdujo en 1993 por IETF, El CIDR es decirenrutamiento sin clase, es la simplificación de red o subredes en una sola dirección Ip que cubra todo ese esquema de direccionamiento Ip. Es lacapacidad que tienen los protocolos de enrutamiento de enviar actualizaciones a sus vecinos de redes con n VLSM, esas direcciones en una sola dirección. Su función es la comunicar varias subredes a través de una sola red general.

Características CIDR.

Permite reducir el número de entradas en una tabla de enrutamiento, agrupando las direcciones mediante el uso de una máscara de 32 bits Enrutamiento inter-dominio sin clase consiste en la capacidad de un enrutador de usar protocolos que no consideran las clases como los límites naturales de las subredes. Tiene en cuenta el direccionamiento VLSM en sus actualizaciones.

Implementación CIDR

Se crea para no desperdiciar Ips y facilitar el envió de Direcciones IPs

# UNIDAD IV

# CAPA DE ENLACE DE DATOS

La capa de enlace de datos proporciona tránsito de datos confiable a través de un enlace físico. Al hacerlo, la capa se ocupa del direccionamiento físico (comparado con el lógico) , la topología de red, el acceso a la red, la notificación de errores, entrega ordenada de tramas y control de flujo. Si desea recordar la Capa 2 en la menor cantidad de palabras posible, piense en tramas y control de acceso al medio.

Una trama por lo más general que sea, incluye:
Datos: El paquete desde la Capa de red que contiene el cuerpo del mensaje encapsulado.
Encabezado: Contiene información de control como direccionamiento y está ubicado al comienzo de la trama.
Tráiler: Contiene información de control agregada al final de la trama.

Cuando los datos viajan por los medios, se convierten en un stream de bits, o en 1 y 0. Si un nodo terminal está recibiendo streams de bits largos ¿cómo determina dónde comienza y termina la trama o qué bits representan una dirección?

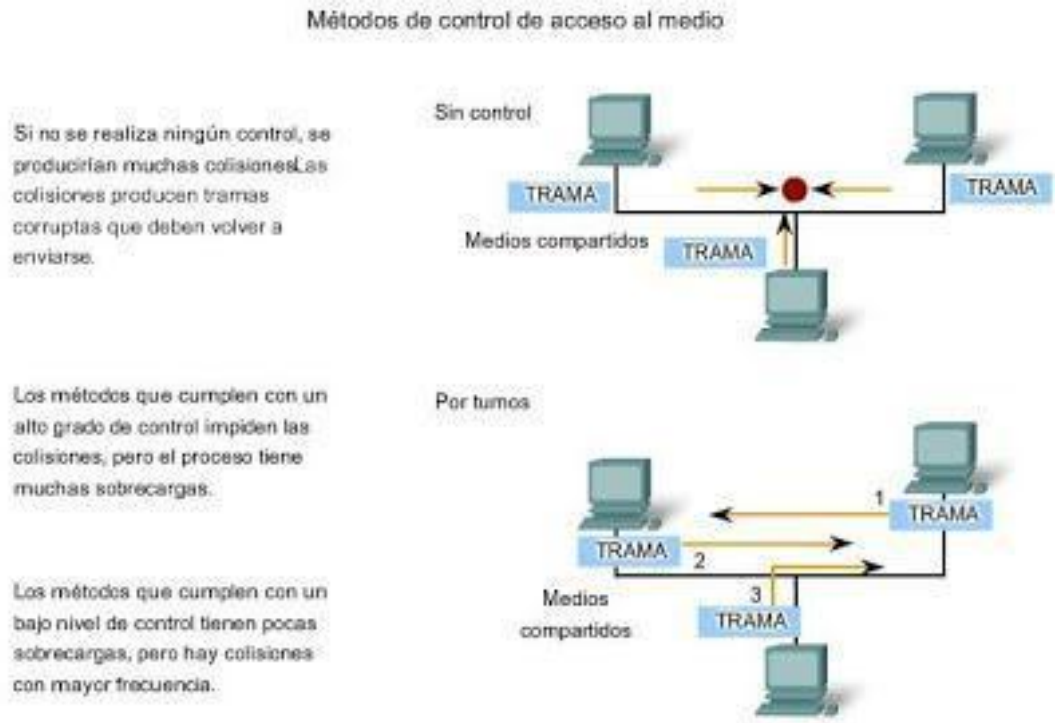
El tramado rompe el stream en agrupaciones descifrables, con la información de control insertada en el encabezado y tráiler como valores en campos diferentes. Este formato brinda a las señales físicas una estructura que puede ser recibida por los nodos y decodificada en paquetes en el destino.

## 4.1 TÉCNICAS DE CONTROL DE ACCESO AL MEDIO

La regulación de la colocación de tramas de datos en los medios es conocida como control de acceso al medio. Entre las diferentes implementaciones de los protocolos de la capa de

enlace de datos, hay diferentes métodos de control de acceso a los medios. Estas técnicas de control de acceso al medio definen si los nodos comparten los medios y de qué manera lo hacen.

El control de acceso al medio es el equivalente a las reglas de tráfico que regulan la entrada de vehículos a una autopista. La ausencia de un control de acceso al medio sería el equivalente a vehículos ignorando el resto del tráfico e ingresando al camino sin tener en cuenta a los otros vehículos.




Sin embargo, no todos los caminos y entradas son iguales. El tráfico puede ingresar a un camino confluyendo, esperando su turno en una señal de parada o respetando el semáforo. Un conductor sigue un conjunto de reglas diferente para cada tipo de entrada. De la misma manera, hay diferentes formas de regular la colocación de tramas en los medios. Los protocolos en la capa de enlace de datos definen las reglas de acceso a los diferentes medios. Algunos métodos de control de acceso al medio utilizan procesos altamente controlados para asegurar que las tramas se coloquen con seguridad en los medios. Estos métodos se definen mediante protocolos sofisticados, que requieren mecanismos que introducen sobrecargas a la red.

El método de control de acceso al medio utilizado depende de:

Compartir medios: si y cómo los nodos comparten los medios.

Topología: cómo la conexión entre los nodos se muestra a la capa de enlace de datos.

## 4.2 MEDIOS COMPARTIDOS

Algunas topologías de red comparten un medio común con varios nodos. En cualquier momento puede haber una cantidad de dispositivos que intentan enviar y recibir datos utilizando los medios de red. Hay reglas que rigen cómo esos dispositivos comparten los medios.

Hay dos métodos básicos de control de acceso al medio para medios compartidos:

Controlado: Cada nodo tiene su propio tiempo para utilizar el medio

Basado en la contención: Todos los nodos compiten por el uso del medio

## 4.3 MEDIOS NO COMPARTIDOS

Los protocolos de control de acceso al medio para medios no compartidos requieren poco o ningún control antes de colocar tramas en los medios. Estos protocolos tienen reglas y procedimientos más simples para el control de acceso al medio. Tal es el caso de las topologías punto a punto.

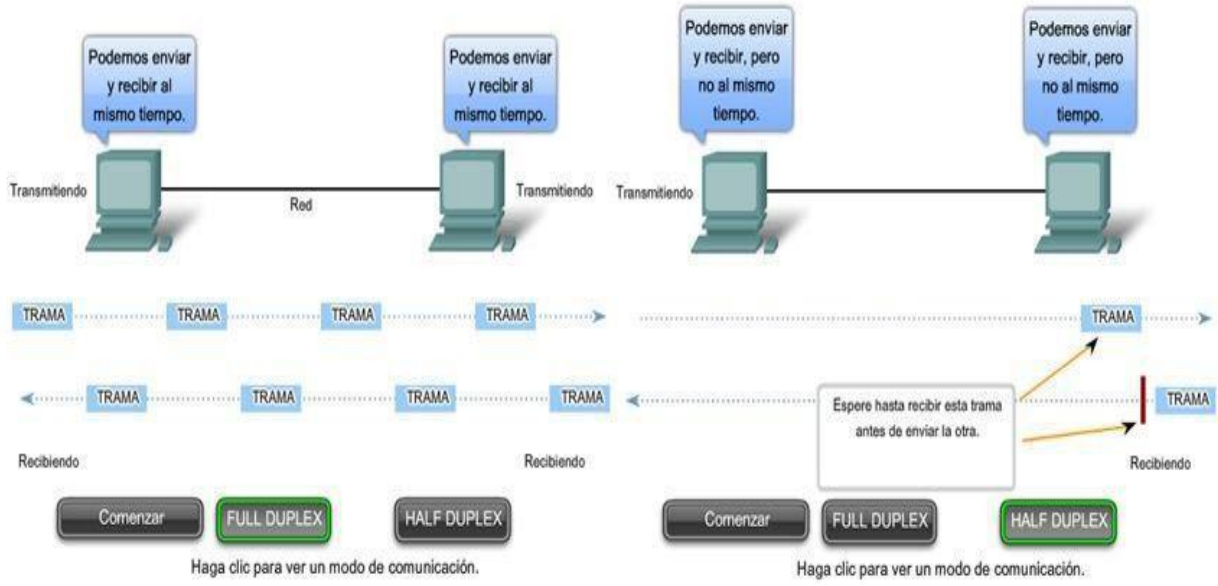
En las topologías punto a punto, los medios interconectan sólo dos nodos. En esta configuración, los nodos no necesitan compartir los medios con otros hosts ni determinar si una trama está destinada para ese nodo. Por lo tanto, los protocolos de capa de enlace de datos hacen poco para controlar el acceso a medios no compartidos.

## Full Duplex y Half Duplex

Comunicación half-duplex quiere decir que los dispositivos pueden transmitir y recibir en los medios pero no pueden hacerlo simultáneamente. Ethernet ha establecido reglas de arbitraje para resolver conflictos que surgen de instancias donde más de una estación intenta transmitir al mismo tiempo.

En la comunicación full-duplex, los dos dispositivos pueden transmitir y recibir en los medios al mismo tiempo. La capa de enlace de datos supone que los medios están disponibles para

transmitir para ambos nodos en cualquier momento. Por lo tanto, no hay necesidad de arbitraje de medios en la capa de enlace de datos.



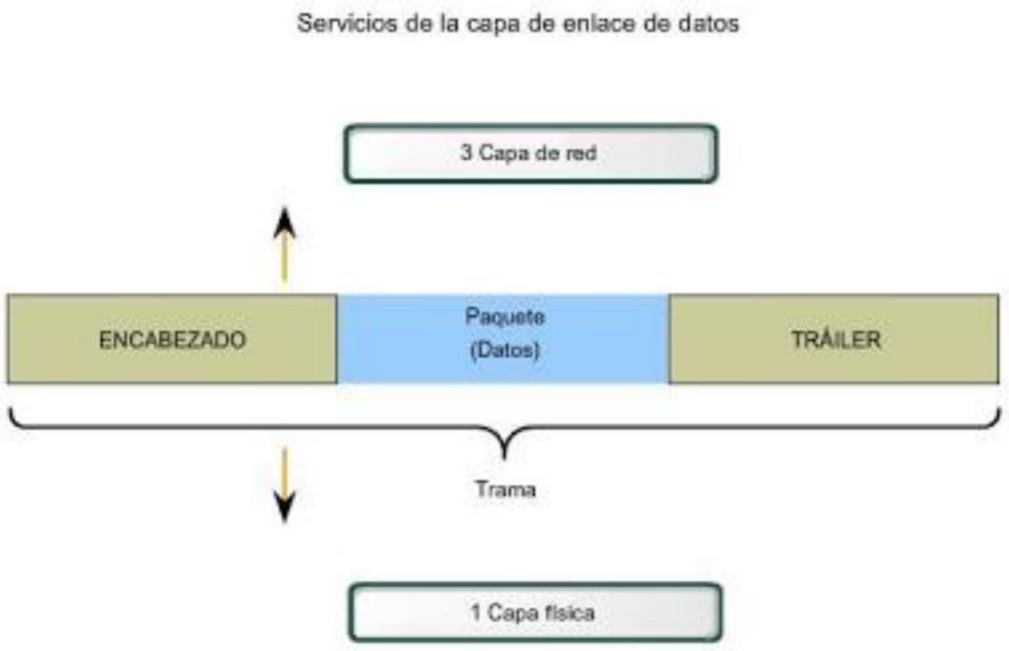

## 4.4 DIRECCIONAMIENTO DEL CONTROL DE ACCESO AL MEDIO Y TRAMADO DE DATOS

La descripción de una trama es un elemento clave de cada protocolo de capa de enlace de datos. Los protocolos de capa de enlace de datos requieren información de control para permitir que los protocolos funcionen. La información de control puede indicar: Qué nodos están en comunicación con otros

Cuándo comienza y cuándo termina la comunicación entre nodos individuales

Qué errores se producen mientras los nodos se comunican

Qué nodos se comunicarán luego




La Capa de enlace de datos prepara un paquete para transportar a través de los medios locales encapsulándolo con un encabezado y un tráiler para crear una trama. A diferencia de otros PDU que han sido analizados en este curso, la trama de la capa de enlace de datos incluye:

Datos: El paquete desde la Capa de red

Encabezado: contiene información de control como direccionamiento y está ubicado al comienzo del PDU

Tráiler: contiene información de control agregada al final del PDU

## 4.5 Estándares

A diferencia de los protocolos de las capas superiores del conjunto TCP/IP, los protocolos de capa de enlace de datos generalmente no están definidos por solicitudes de comentarios (RFC). A pesar de que el Grupo de trabajo de ingeniería de Internet (IETF) mantiene los protocolos y servicios funcionales para la suite de protocolos TCP/IP en las capas superiores, la IETF no define las funciones ni la operación de esa capa de acceso a la red del modelo. La

capa de acceso de red TCP/IP es el equivalente de las capas de enlace de datos OSI y la física. Estas dos capas se verán en capítulos separados para un análisis más detallado.

Los protocolos y servicios funcionales en la Capa de enlace de datos son descriptos por organizaciones de ingeniería (como IEEE, ANSI y ITU) y compañías en comunicaciones. Las organizaciones de ingeniería establecen estándares y protocolos públicos y abiertos. Las compañías de comunicaciones pueden establecer y utilizar protocolos propios para aprovechar los nuevos avances en tecnología u oportunidades de mercado.

Los servicios y especificaciones de la capa de enlace de datos se definen mediante varios estándares basados en una variedad de tecnologías y medios a los cuales se aplican los protocolos. Algunos de estos estándares integran los servicios de la Capa 2 y la Capa 1.

Las organizaciones de ingeniería que definen estándares y protocolos abiertos que se aplican a la capa de enlace de datos incluyen:

Organización Internacional para la Estandarización (ISO)

Instituto de Ingenieros Eléctricos y Electrónicos (IEEE)

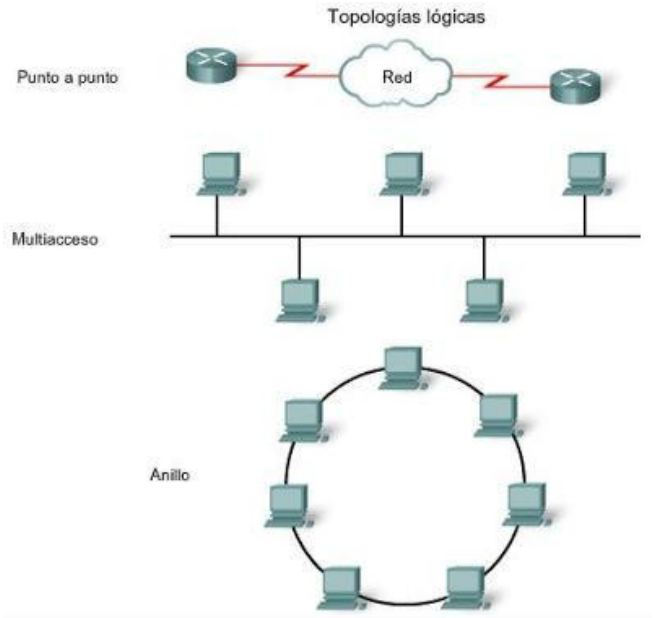
Instituto Nacional Estadounidense de Estándares (ANSI)

Unión Internacional de Telecomunicaciones (ITU)

Estándares para la capa de enlace de datos

| | |
|---|---|
| ISO: | HDLC (Control de enlace de datos de alto nivel) |
| IEEE: | 802.2 (LLC),<br>802.3 (Ethernet)<br>802.5 (Token Ring)<br>802.11(Wireless LAN [LAN inalámbrico]) |
| ITU: | Q.922 (Estándar de Frame Relay)<br>Q.921 (Estándar de enlace de datos ISDN)<br>HDLC (Control de enlace de datos de alto nivel) |
| ANSI: | 3T9.5<br>ADCCP (Protocolo de control de comunicación avanzada de datos) |

## 4.6 COMPARACIÓN ENTRE TOPOLOGÍA LÓGICA Y FÍSICA



La topología de una red es la configuración o relación de los dispositivos de red y las interconexiones entre ellos. Las topologías de red pueden verse en el nivel físico y el nivel lógico.
La topología física es una configuración de nodos y las conexiones físicas entre ellos. La representación de cómo se usan los medios para interconectar los dispositivos es la topología física. Ésta se abarcará en capítulos posteriores de este curso.

Una topología lógica es la forma en que una red transfiere tramas de un nodo al siguiente. Esta configuración consiste en conexiones virtuales entre los nodos de una red independiente de su distribución física. Los protocolos de capa de enlace de datos definen estas rutas de señales lógicas. La capa de enlace de datos "ve" la topología lógica de una red al controlar el acceso de datos a los medios. Es la topología lógica la que influye en el tipo de trama de red y control de acceso a medios utilizados.

**Comparacion entre la topologia logica y la topologia**
**fisica** Comparacion entre la topologia logica y la topologia fisica
La topología de una red es la configuración o relación de los dispositivos de red y de las interconexiones entre ellos. Las topologías de red pueden verse en el nivel físico y en el nivel lógico.

La topología física es una configuración de nodos y las conexiones físicas entre ellos. La representación de cómo se usan los medios para interconectar los dispositivos es la topología física. Esto se abarcará en capítulos posteriores de este curso.

Una topología lógica es la forma en que una red transfiere tramas de un nodo al siguiente. Esta configuración consiste en conexiones virtuales entre los nodos de una red independiente de su distribución física. Los protocolos de capa de enlace de datos definen estas rutas de señales lógicas. La capa de enlace de datos "ve" la topología lógica de una red

al controlar el acceso de datos a los medios. Es la topología lógica la que influye en el tipo de trama de red y control de acceso a los medios que se utilizan.

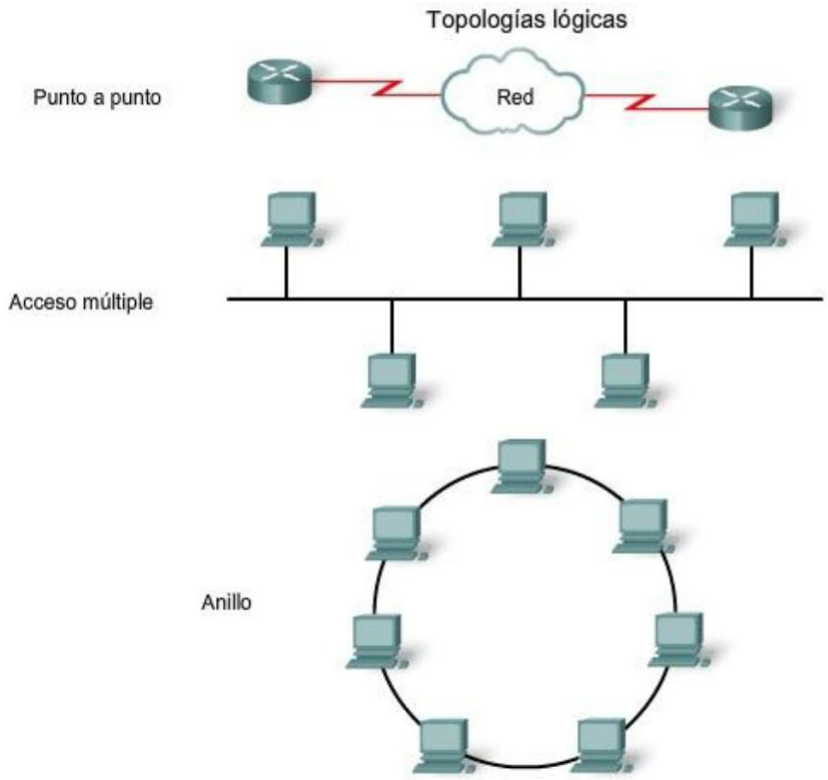
La topología física o cableada de una red probablemente no sea la misma que la topología lógica.

La topología lógica de una red está estrechamente relacionada con el mecanismo que se utiliza para administrar el acceso a la red. Los métodos de acceso proporcionan los procedimientos para administrar el acceso a la red para que todas las estaciones tengan acceso. Cuando varias entidades comparten los mismos medios, deben estar instalados algunos mecanismos para controlar el acceso. Los métodos de acceso son aplicados a las redes para regular este acceso a los medios. Los métodos de acceso se analizarán con más detalle más adelante.

Las topologías lógica y física generalmente utilizadas en redes son:

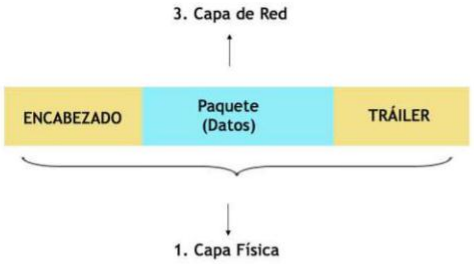
- Punto a Punto
- Acceso múltiple
- Anillo

Las implementaciones lógicas de estas topologías y sus métodos asociados de control de acceso al medio se tratan en las siguientes secciones

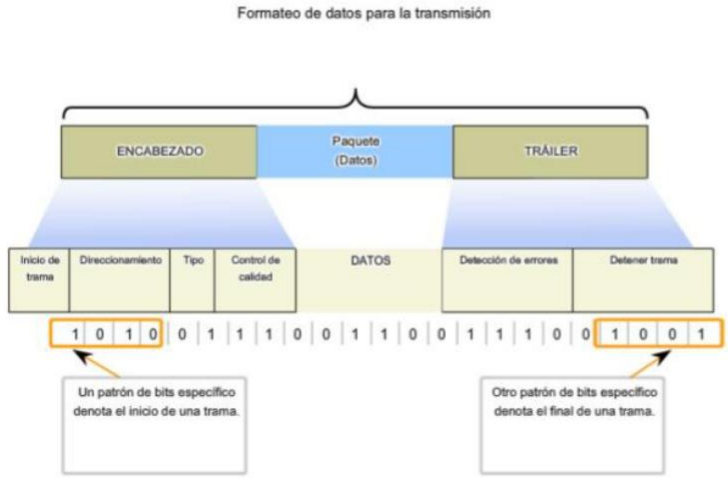



La capa de enlace de datos existe como una capa de conexión entre los procesos de software de las capas por encima de ella y la capa física debajo de ella. Como tal, prepara los paquetes de capa de red para la transmisión a través de alguna forma de medio, ya sea cobre, fibra o entornos /medios inalámbricos.

En muchos casos, la Capa de enlace de datos está incorporada en una entidad física como tarjeta de interfaz de red (NIC) de Ethernet, que se inserta dentro del bus del sistema de una computadora, switch o router y hace la conexión entre los procesos de software que se ejecutan en los dispositivos finales y los medios físicos. Sin embargo, la NIC no es solamente una entidad física. El software asociado con la NIC permite que la NIC realice sus funciones de intermediara preparando los datos para la transmisión y codificando los datos como señales que deben enviarse sobre los medios asociados.




## Formateo de los datos para la Transmisión




Señales de Comunicación

La capa física de OSI proporciona los medios de transporte para los bits que conforman la trama de la capa de Enlace de datos a través de los medios de red. Esta capa acepta una trama completa desde la capa de Enlace de datos y lo codifica como una secuencia de señales que se transmiten en los medios locales. Un dispositivo final o un dispositivo intermedio recibe los bits codificados que componen una trama.

El envío de tramas a través de medios de transmisión requiere los siguientes elementos de la capa física:

- Medios físicos y conectores asociados.
- Una representación de los bits en los medios.

- Codificación de los datos y de la información de control.
- Sistema de circuitos del receptor y transmisor en los dispositivos de red.

En este momento del proceso de comunicación, la capa de transporte ha segmentado los datos del usuario, la capa de red los ha colocado en paquetes y luego la capa de enlace de datos los ha encapsulado como tramas. El objetivo de la capa física es crear la señal óptica, eléctrica o de microondas que representa a los bits en cada trama. Luego, estas señales se envían por los medios una a la vez.

Otra función de la capa física es la de recuperar estas señales individuales desde los medios, restaurarlas para sus representaciones de bit y enviar los bits hacia la capa de Enlace de datos como una trama completa

## 4.7 SEÑALIZACIÓN Y CODIFICACIÓN FÍSICA

Las tres funciones esenciales de la capa física son:

- Los componentes físicos
- Codificación de datos
- Señalización

Los elementos físicos son los dispositivos electrónicos de hardware, medios y conectores que transmiten y transportan las señales para representar los bits.

### 4.8 CODIFICACIÓN

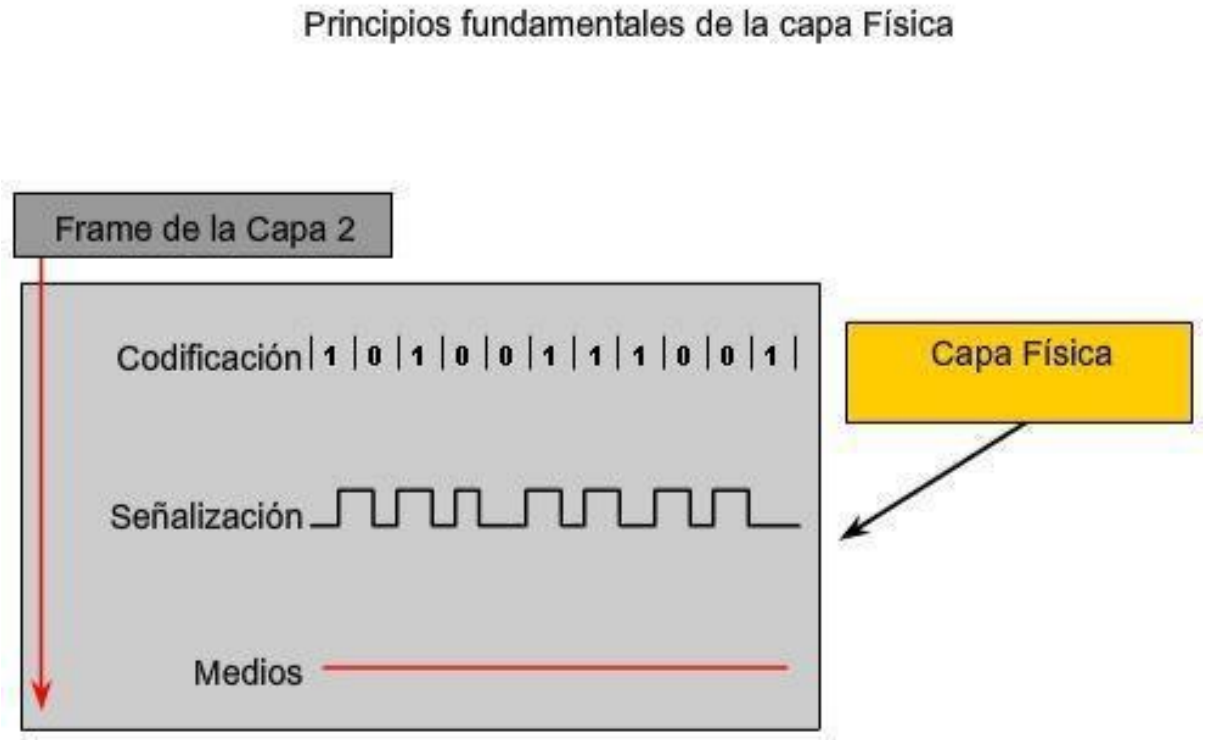
La codificación es un método utilizado para convertir un stream de bits de datos en un código predefinido. Los códigos son grupos de bits utilizados para ofrecer un patrón predecible que pueda reconocer tanto el emisor como el receptor. La utilización de patrones predecibles permite distinguir los bits de datos de los bits de control y ofrece una mejor detección de errores en los medios.

Además de crear códigos para los datos, los métodos de codificación en la capa física también pueden proporcionar códigos para control, como la identificación del comienzo y el

final de una trama. El host que realiza la transmisión transmitirá el patrón específico de bits o un código para identificar el comienzo y el final de la trama.

## Señalización

La capa física debe generar las señales inalámbricas, ópticas o eléctricas que representan el "1" y el "0" en los medios. El método de representación de bits se denomina método de señalización. Los estándares de capa física deben definir qué tipo de señal representa un "1" y un "0". Esto puede ser tan sencillo como un cambio en el nivel de una señal eléctrica, un impulso óptico o un método de señalización más complejo.



## Representación Gráfica de las Redes

Encontraremos en este campo de estudio, que para poder diseñar redes se necesita tener una simbología para cada componente, en la siguiente imagen veremos algunos ejemplos.


Además de estas representaciones, se utiliza terminología especializada al hablar sobre cómo se conectan estos dispositivos unos a otros.

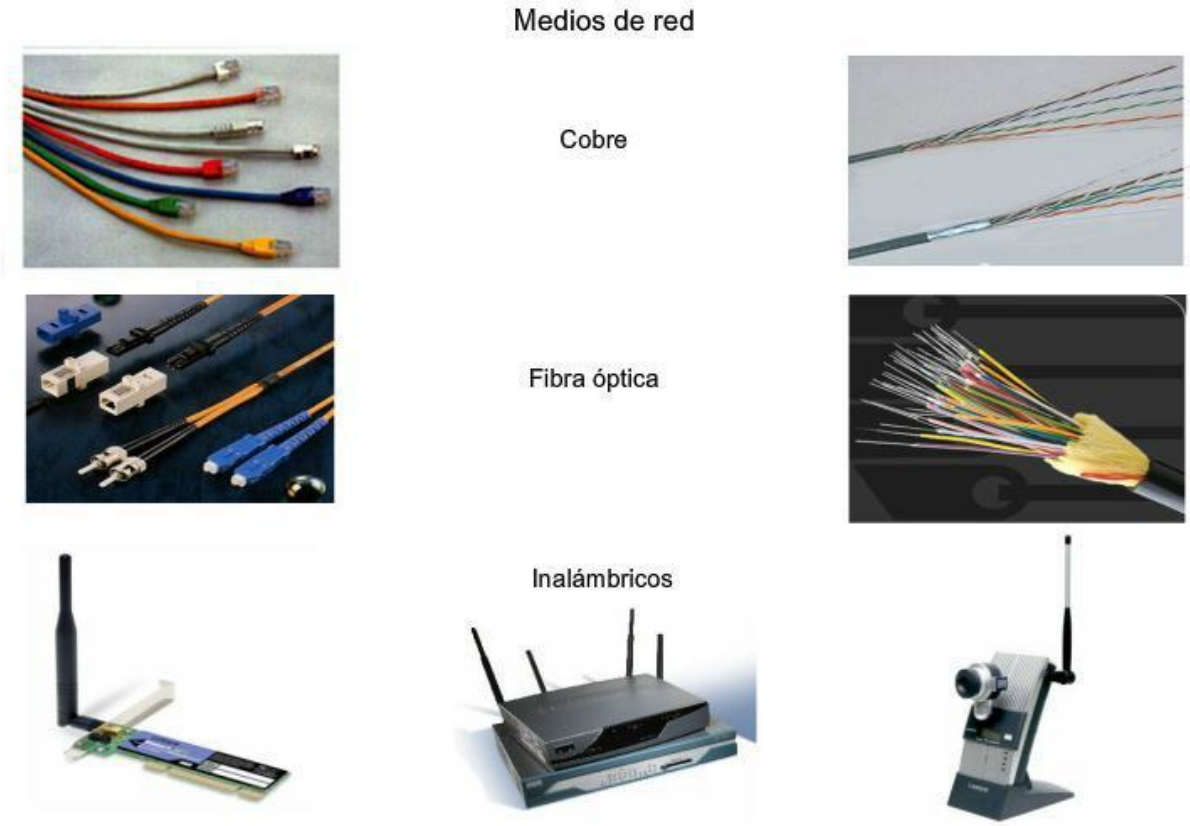
- **Tarjeta de interfaz de red:** una NIC, o adaptador LAN, proporciona la conexión física a la red para la PC u otro dispositivo host. Los medios que realizan la conexión de la PC al dispositivo de red se conectan en la NIC.
- **Puerto físico:** se trata de un conector o una boca en un dispositivo de red donde se conectan los medios a un host u otro dispositivo de red.

**Interfaz:** puertos especializados en un dispositivo de internetworking que se conectan a redes individuales. Puesto que los routers se utilizan para interconectar redes, los puertos de un router se conocen como interfaces de red.

**Medios de transmisión**

El medio de transmisión constituye el soporte físico a través del cual emisor y receptor pueden comunicarse en un sistema de transmisión de datos. Las redes modernas utilizan principalmente tres tipos de medios para interconectar los dispositivos y proporcionar la ruta por la cual pueden transmitirse los datos. Estos medios son:

- hilos metálicos dentro de los cables
- fibras de vidrio o plásticas (cable de fibra óptica)
- transmisión inalámbrica.




La codificación de señal que se debe realizar para que el mensaje sea transmitido es diferente para cada tipo de medio. En los hilos metálicos, los datos se codifican dentro de impulsos

eléctricos que coinciden con patrones específicos. Las transmisiones por fibra óptica dependen de pulsos de luz, dentro de intervalos de luz visible o infrarroja. En las transmisiones inalámbricas, los patrones de ondas electromagnéticas muestran los distintos valores de bits.

Distinguimos dos tipos de medios: guiados y no guiados. Los medios guiados conducen (guían) las ondas a través de un camino físico. Los medios no guiados proporcionan un soporte para que las ondas se transmitan a través de aire o el vacío. Estos medios se dividen en:

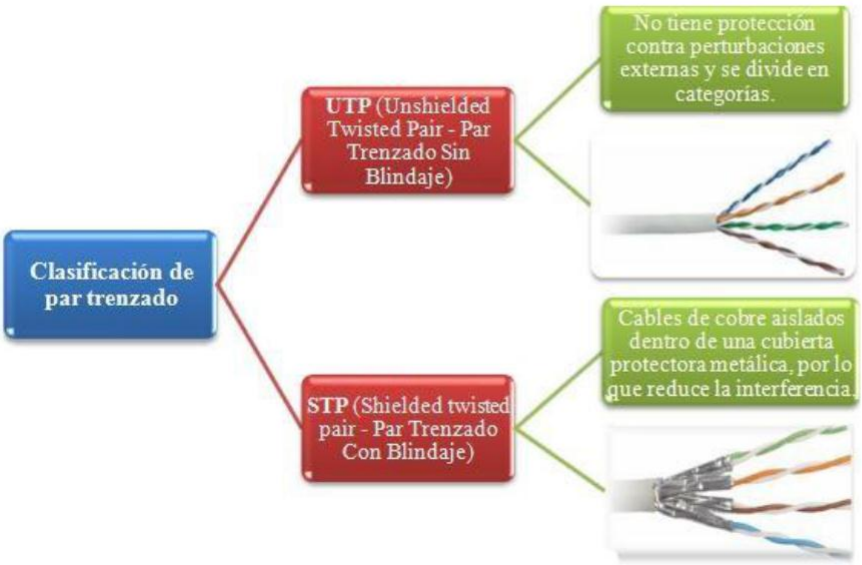
- **Medios guiados**
  - **Par trenzado**
  - **Cable coaxial**
  - **Fibra óptica**

- **Medios no guiados**
  - **Radiofrecuencias**
  - **Microondas**
  - **Infrarrojos**

## 4.9 MEDIOS GUIADOS.

Son aquellos cuya señal está viajando por cualquiera de estos medios es dirigida y contenida por los límites físicos del medio. El par trenzado y el cable coaxial usan conductores metálicos que transportan señales de corriente eléctrica. La fibra óptica es un cable de cristal o plástico que acepta y transporta señales en forma de luz. Par trenzado

Este consiste en dos alambres de cobre aislados, en general de 1mm de espesor. Los alambres se entrelazan en forma helicoidal, como en una molécula de DNA. La forma trenzada del cable se utiliza para reducir la interferencia eléctrica con respecto a los pares cercanos que se encuentran a su alrededor. Los pares trenzados se pueden utilizar tanto para transmisión analógica como digital, y su ancho de banda depende del calibre del alambre y de la distancia que recorre. Estos utilizan conectores RJ-45.




Los UTP se manejan en distintas categorias que seran mostradas a continuación:

| TIPO | CARACTERÍSTICAS |
|---|---|
| **Categoría 1** | Alcanza como máximo una velocidad de 100 Kbps. Se utiliza en redes telefónicas. |
| **Categoría 2** | Este cable consta de 4 pares trenzados de hilo de cobre. Las características de transmisión del medio están especificadas hasta una frecuencia de 4 MHz. |
| **Categoría 3** | Velocidad de transmisión de 10 Mbps para Ethernet. Se implementan las redes Ethernet 10BaseT y trabaja a una frecuencia superior de 16 MHz. |
| **Categoría 4** | Velocidad de transmisión de 20 Mbps. Usada para redes Token Ring. |
| **Categoría 5** | Transmite datos hasta 100Mbps a una frecuencia superior de 100 MHz. Es empleado para redes LAN. |
| **Categoría 5e** | Es la categoría 5 mejorada. Minimiza la atenuación y las interferencias. Es la más utilizada actualmente. |
| **Categoría 6** | Transmite datos hasta 1Gbps a una frecuencia superior a 250 MHz. |

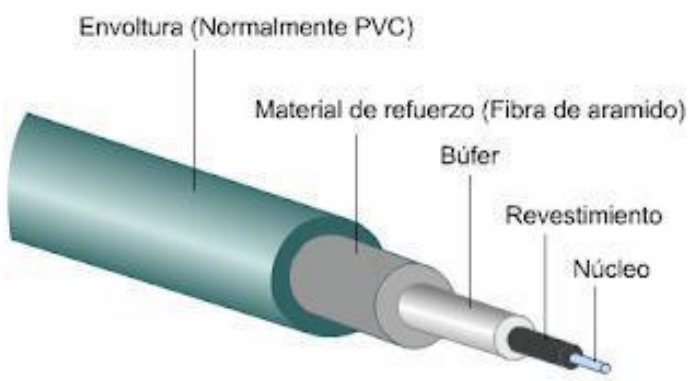
## 4.10 CABLE COAXIAL

La velocidad de transmisión que se puede alcanzar con el cable coaxial llega solo hasta 10Mbps dependiendo de la longitud del cable, si utilizamos un cable delgado se puede transmitir más rápido, en cambio con un cable más grueso la transmisión es más lenta. El cable coaxial consta de un alambre de cobre duro en su parte central, es decir, que constituye el núcleo, el cual se encuentra rodeado por un material aislante. Este material

aislante está rodeado por un conductor cilíndrico que frecuentemente se presenta como una malla de tejido trenzado. El conductor externo está cubierto por una capa de plástico protector. Que ofrece una excelente inmunidad al ruido.

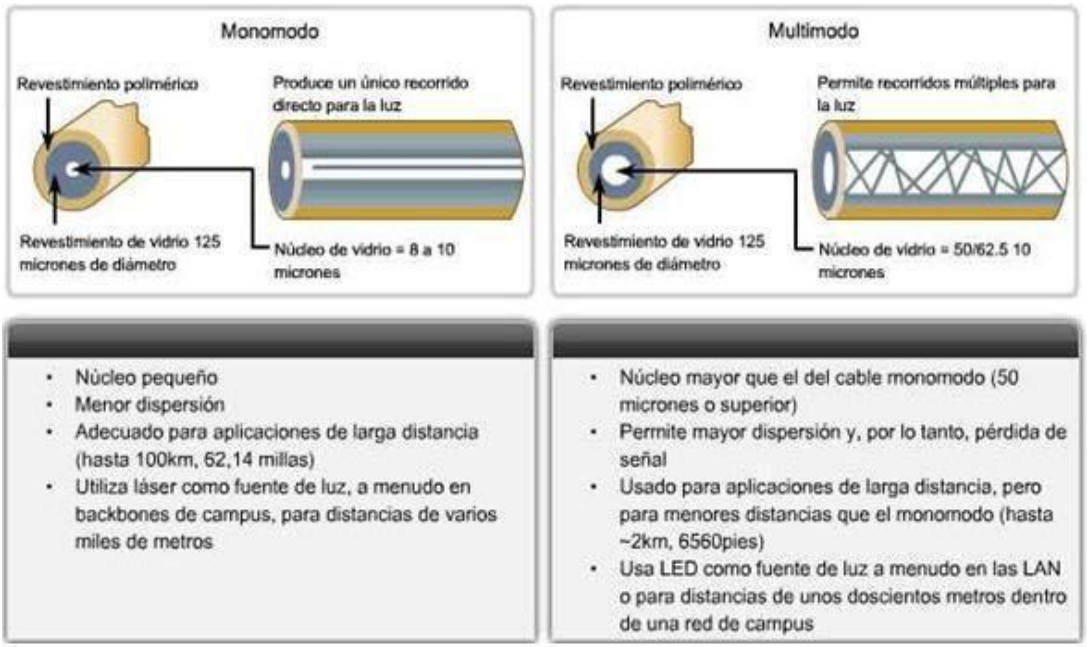

## 4.11 FIBRA ÓPTICA

Un cable de fibra óptica consta de tres secciones concéntricas. La más interna, el núcleo, consiste en una o más hebras o fibras hechas de cristal o plástico. Cada una de ellas lleva un revestimiento de cristal o plástico con propiedades ópticas distintas a las del núcleo. La capa más exterior, que recubre una o más fibras, debe ser de un material opaco y resistente.




Un sistema de transmisión por fibra óptica está formado por una fuente luminosa muy monocromática (generalmente un láser), la fibra encargada de transmitir la señal luminosa y un fotodiodo que reconstruye la señal eléctrica. La luz que se mueve por el núcleo debe ser reflejada por cubierta y no refractada en ella. Tiene 2 métodos de propagación multimodo y

monomodo; y la primera se puede implementar de 2 maneras: índice escalonado o índice de gradiente gradual.




## Medios no guiados

Los medios no guiados o comunicación sin cable transportan ondas electromagnéticas sin usar un conductor físico, sino que se radian a través del aire, por lo que están disponibles para cualquiera que tenga un dispositivo capaz de aceptarlas.

Los medios no guiados han tenido gran acogida al ser un buen medio de cubrir grandes distancias y hacia cualquier dirección, su mayor logro se dio desde la conquista espacial a través de los satélites y su tecnología no para de cambiar. De manera general podemos definir las siguientes características de este tipo de medios: La transmisión y recepción se realiza por medio de antenas, las cuales deben estar alineadas cuando la transmisión es direccional, o si es omnidireccional la señal se propaga en todas las direcciones.

## Radio enlaces de VHF y UHF

Estas bandas cubren aproximadamente desde 55 a 550 MHz. Son también omnidireccionales, pero a diferencia de las anteriores la ionosfera es transparente a ellas. Su alcance máximo es

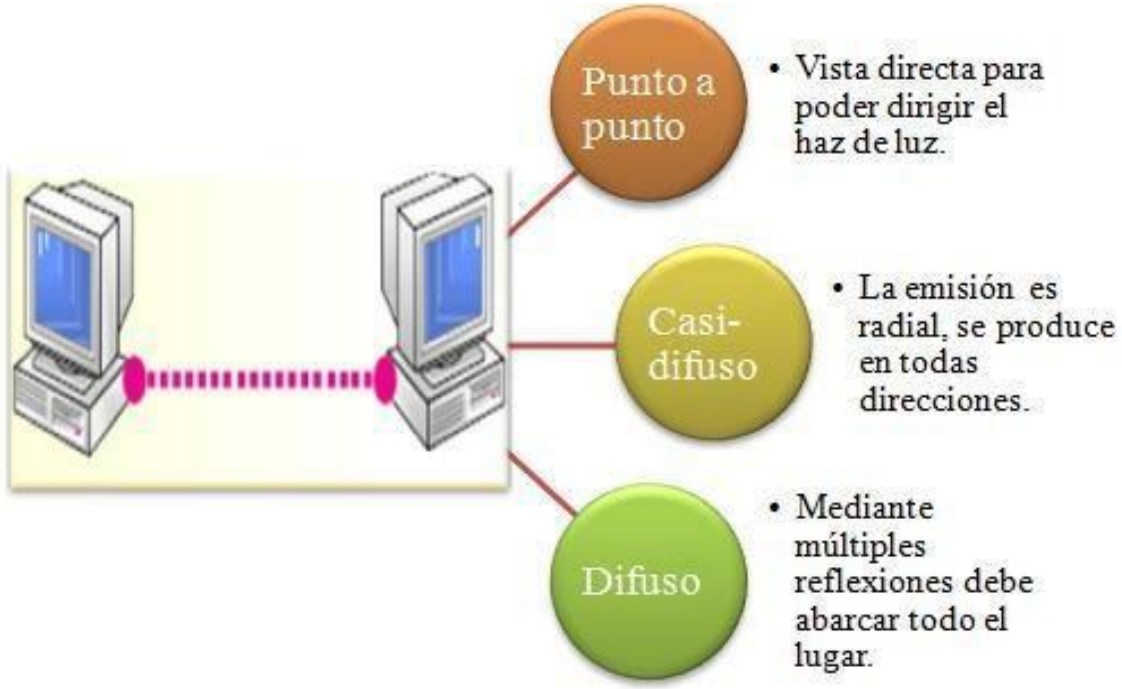
de un centenar de kilómetros, y las velocidades que permite del orden de los 9600 bps. Su aplicación suele estar relacionada con los radioaficionados y con equipos de comunicación militares, también la televisión y los aviones.

## Microondas

Las microondas nos permiten transmisiones tanto terrestres como con satélites. Dada sus frecuencias, del orden de 1 a 10 GHz, las microondas son muy direccionales y sólo se pueden emplear en situaciones en que existe una línea visual que une emisor y receptor. Los enlaces de microondas permiten grandes velocidades de transmisión, del orden de 10 Mbps.

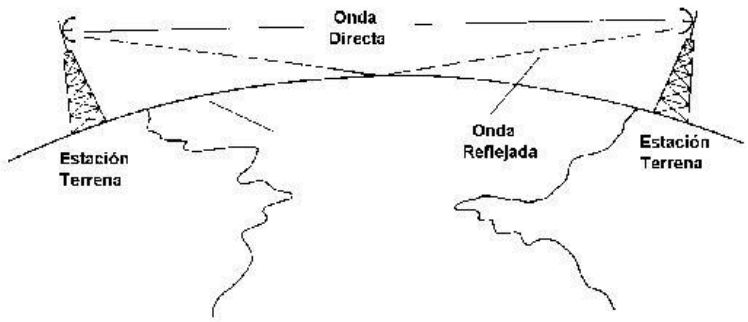
## Infrarrojos

Utilizan un haz de luz infrarroja que transporta los datos entre dispositivos. Debe existir visibilidad directa entre los dispositivos que transmiten y los que reciben ya que de lo contrario se puede ver interrumpida la comunicación. Existen 3 modos de transmisión:



## Microondas Terrestres

Los sistemas de microondas terrestres han abierto una puerta a los problemas de transmisión de datos, sin importar cuales sean, aunque sus aplicaciones no estén restringidas a este campo solamente. 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 varia 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.



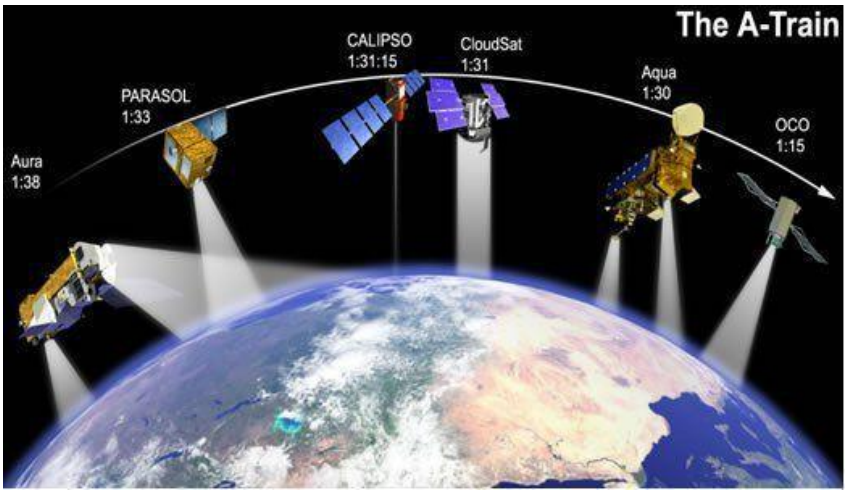

Enlace de Microondas de Linea de Vista

Para la comunicación de microondas terrestres 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.

## 4.12 SATÉLITES

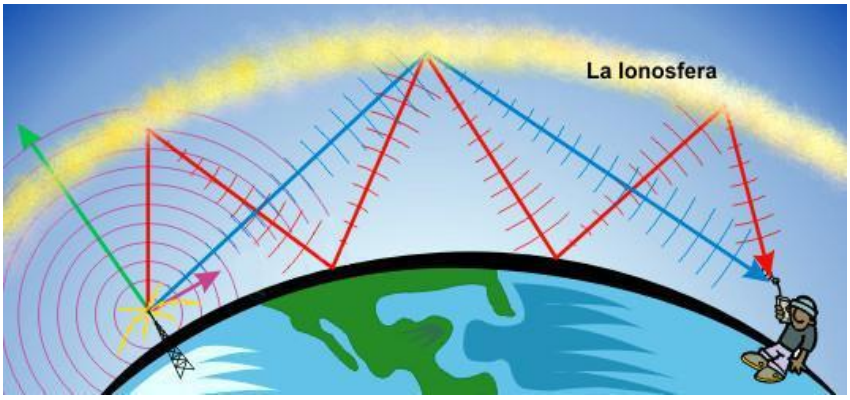
Conocidas como microondas por satélite, esta basado en la comunicación llevada a cabo a través de estos dispositivos, los cuales después de ser lanzados de la tierra y ubicarse en la orbita terrestre siguiendo las leyes descubiertas por Kepler, realizan la transmisión de todo tipo de datos, imágenes, 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.




## 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 usados por determinadas redes de datos o los infrarrojos.



## **BIBLIOGRAFÍA**:


El modelo OSI, Recuperado de: http://www.tecnotopia.com.mx/redes/redosi.htm

El modelo OSI, recuperado de: http://www.tecnotopia.com.mx/redes/redosi.htm

Redes De Computadoras, recuperado de: https://sites.google.com/site/investigacionesitlm/

Manejo de subredes, recuperado de: https://sites.google.com/site/redescarlosvillegas/unidad-iii/3-1-capa-de-red/3-1-4-direccionamiento-ip/3-1-4-2-manejo-de-subredes

Introducción al conjunto de protocolos TCP/IP, recuerado de: https://docs.oracle.com/cd/E19957-01/820-2981/6nei0r0r9/index.html

Arquitectura en Capas, recuperado de: https://reactiveprogramming.io/blog/es/estilos-arquitectonicos/capas

VLSM y CIDR, recuperado de: https://sites.google.com/site/redescarlosvillegas/unidad-iii/3-1-capa-de-red/3-1-4-direccionamiento-ip/3-1-4-4-vlsm-y-cidr

Qué es el direccionamiento IP y cómo funciona, Recuperado de: https://www.profesionalreview.com/2019/01/12/direccionamiento-ip/

Enrutamiento y sus características, Recuperado de: https://sites.google.com/site/redesdecomputadorashamed/unidad-3-capas-inferiores-del-modelo-osi-y-tcp-ip/3-1-capa-de-red/3-1-3-enrutamiento-y-sus-caracteristicas

Redes de computadoras, Quinta edición, ANDREW S. TANENBAUM y DAVID J. WETHERALL, PEARSON EDUCACIÓN, México, 2012

Capa de enlace de datos, recuperado de: https://sites.google.com/site/sabyrodriguezgamez/unidad-iii/3-2-capa-de-enlace-de-datos

Otras fuentes:

http://neo.lcc.uma.es/evirtual/cdd/tutorial/fisico/Mtransm.html

https://sites.google.com/site/sistemasdemultiplexado/arquitecturas-de-las-redes-de--comunicacin-caractersticas/7--medios-de-transmisin-de-datos

http://socializandoredes.blogspot.mx/2012/11/medios-de-transmision-de-datos.html

https://es.wikipedia.org/wiki/Medio_de_transmisi%C3%B3n