UNIVERSIDAD EAN

Workshop 3

Realizado por:

Leonardo Jiménez Ubaque

Willington Andrés Niño Pérez

Alex Buitrago Basallo

Ingeniería de Sistemas

Redes I

Docente

Alexander García Pérez

Bogotá D.C

07 de mayo de 2023

Índice

Introducción

En la era digital en la que vivimos, la sociedad está altamente conectada a la tecnología, es por esto por lo que la transmisión información es parte fundamental de la comunicación que conocemos hoy en día, donde las redes son importantes para esta interconexión global que existe y que a su vez nos permite realizar acciones como lo son la comunicación, entretenimiento, trabajo o educación. Sin embargo, detrás de este proceso de conectividad hay un complejo conjunto de acciones y una infraestructura de redes que permite que nuestros datos sean transferidos de una manera eficiente y segura. Por lo tanto, es importante conocer estos conceptos que son claves en las redes y nos permiten comunicarnos a través de nuestros dispositivos tecnológicos.

En este trabajo, se abordarán y analizaran principalmente tres temas que son parte clave del mundo de las redes y nos permiten transmitir datos para nuestra comunicación, estos son: Modelo OSI (*OSI Model*) "*Open Systems Interconnection*" o en español "*Interconexión de Sistemas Abiertos*", el cual es una herramienta muy importante para el diseño, la implementación y el mantenimiento de las redes; Modelo TCP/IP (*TCP/IP Model*) "*Transmission Control Protocol/Internet Protocol*" o en español "*Protocolo de Control de Transmisión/Protocolo de Internet*", uno de los estándares más usados en la comunicación y que es ampliamente utilizado globalmente; y Sistema de cableado estructurado (Structured Cabling System), una parte esencial para garantizar una comunicación de calidad.

Dado que cada uno de estos temas está detrás de la forma en la que nos comunicamos y estamos conectados. Por lo tanto, son una parte fundamental de la transmisión de datos de forma segura, rápida y eficiente. Es importante conocer cómo funciona cada uno y la forma en la que se aplican para que podamos enviar cualquier tipo de archivo o mensaje desde nuestro computador a otro computador o dispositivo que usamos en nuestra cotidianidad.

Dicho lo anterior, es por esto por lo que a través de este trabajo se espera obtener una mayor comprensión de estos temas tan importantes en el mundo de las redes. De esta manera, se podrá entender de una forma más aproximada en cómo funcionan las redes para nuestra comunicación y cómo podemos aplicar estos conocimientos en nuestra carrera y en la vida diaria.

Modelo OSI (OSI Model)

El modelo OSI ("*Open System Interconnection Model"* o en español "*Modelo de Interconexión de Sistemas Abiertos")* es creado en la década de 1980 por la ISO ("Internacional Organization for Standardization" o en español "Organización Internacional de Normalización"), en estos años existía un problema en cuanto a la comunicación de las computadoras, debido a que existían numerosos fabricantes , compañías y tecnologías en el mundo relacionado a las redes y las telecomunicaciones, donde cada uno realizaba las comunicaciones de sus dispositivos de una manera totalmente diferente. La ISO busco que mediante la creación de un modelo se lograra una estandarización en las comunicaciones digitales, es por esto por lo que se desarrolló el Modelo OSI, el cual es un modelo teórico de referencia que define el cómo se deben diseñar y construir las redes de comunicaciones mediante la aplicación de diferentes protocolos.

El Modelo OSI a parte de ser un estándar en la actualidad también permite una facilidad en la identificación y comprensión de como funciona las comunicaciones. Según Stallings (2013), "el Modelo OSI proporciona un marco conceptual para entender cómo funciona una red" (p. 26). Sin embargo, el Modelo OSI no es ninguna topología de red, ni una especificación de protocolos; es una herramienta que define la funcionalidad de los protocolos, esto para que se logre un estándar de comunicación, para que los diferentes dispositivos logren comunicar información entre sí, es tanta su importancia que si no existiera este modelo el internet que conocemos seria prácticamente imposible. Esta idea es reforzada por Stallings (2013), el cual dice que el objetivo principal del Modelo OSI era brindar un conjunto de normas abiertas y universales que permitieran a los desarrolladores de software y los distintos fabricantes de hardware de redes diseñar y construir productos interconectables e interoperables.

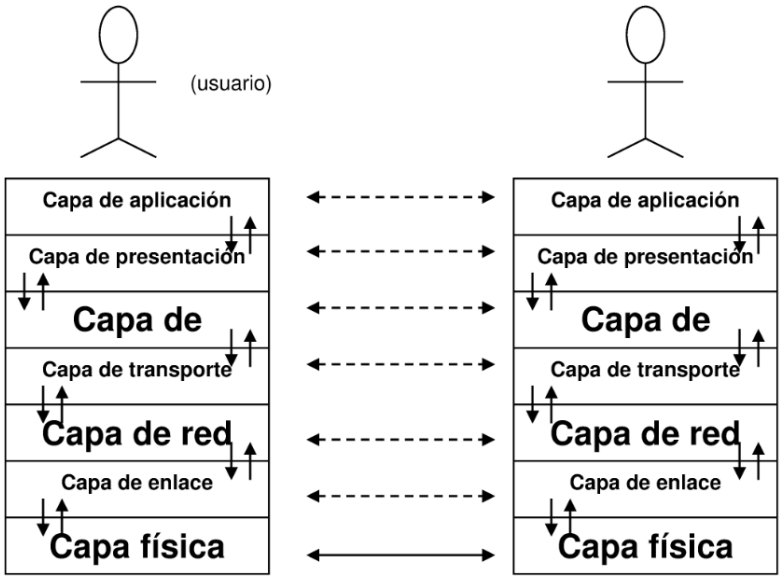

Figura 1.1. Ilustración del Modelo OSI. Tomado de Conceptos de redes de computadoras (p.18), por Caffa, A. (2016).

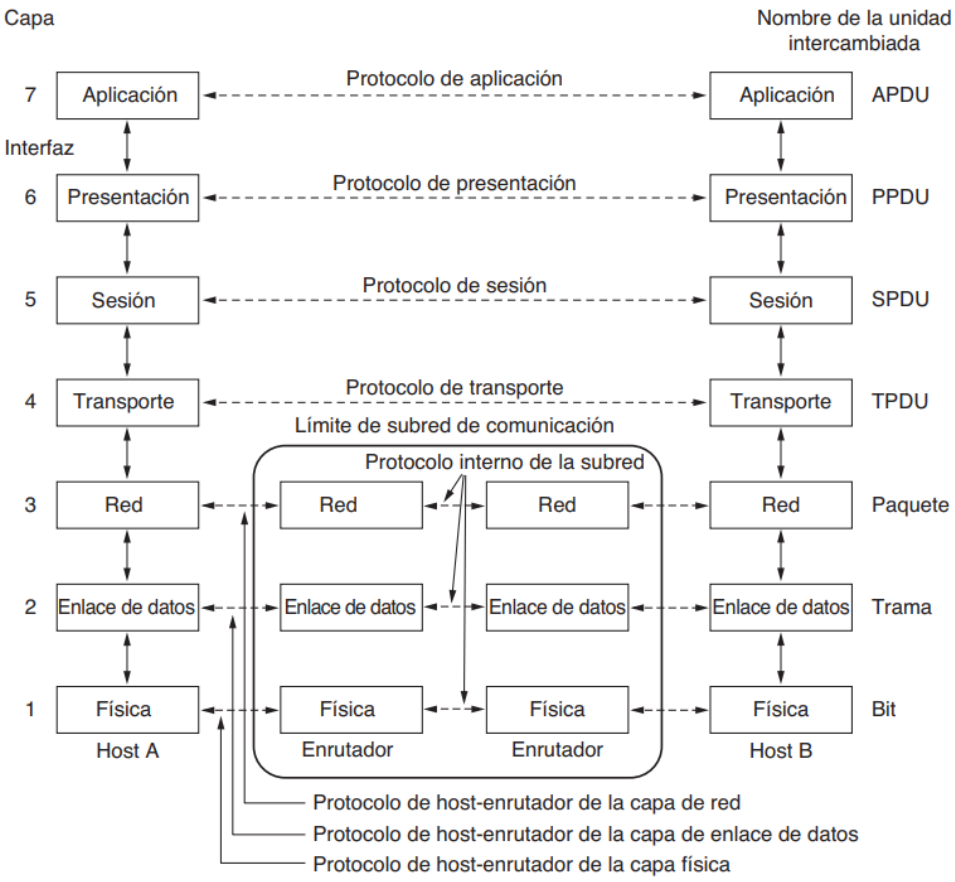

Figura 1.2. Ilustración del Modelo OSI. Tomado de Redes de computadoras (p.36), por Tanenbaum, A. S., & Wetherall, D. J, 2012

Las dos imágenes anteriores son una representación del Modelo OSI, donde nos muestran cómo es la división de este modelo en capas. También, se muestra mediante flechas como puede ser el flujo de la información en este modelo pasando de una capa a otro.

Capas del Modelo OSI

El modelo OSI como se mencionó antes está dividido en capas las cuales permiten las comunicaciones, de acuerdo con Forouzan (2013), este modelo esta basado en un total de siete capas, cada una con una función especifica en la comunicación de datos. Las 7 capas que conforman al Modelo OSI son las siguientes: Capa física, Capa de enlace, Capa de red, Capa de trasporte, Capa de sesión, Capa de presentación y Capa de aplicación.

Esta división del trabajo de las comunicaciones en distintas capas dentro del Modelo OSI se realiza para una mayor facilidad en los sistemas, según Tanenbaum y Wetherall (2012), “el Modelo OSI divide la complejidad de las comunicaciones de red en componentes más pequeños y manejables. Cada capa tiene una función bien definida y

utiliza los servicios proporcionados por la capa inmediatamente inferior para implementar su propia funcionabilidad" (p.77).

A continuación, se presentan dos imágenes que describen el proceso por pasos para realizar un viaje en avión, se puede observar que para que un paso ocurra primero debe pasar otro, es decir si queremos embarcar un avión primero debemos hacer la facturación del equipaje, pero para poder realizar este proceso primero se debe comprar el billete o boleto. De acuerdo con el ejemplo presentado, podemos relacionar este ejemplo con el funcionamiento del Modelo OSI, podemos tomas los pasos que se ven en la imagen como si fueran las capas del modelo, la capa superior seria la capa de aplicación donde queremos que nuestra información viaje desde nuestro equipo hacia otro, y para esto deberá completar una serie de pasos, los cuales dependen de que se cumpla cada uno para una comunicación efectiva, esta seria una breve aproximación del funcionamiento del Modelo OSI.

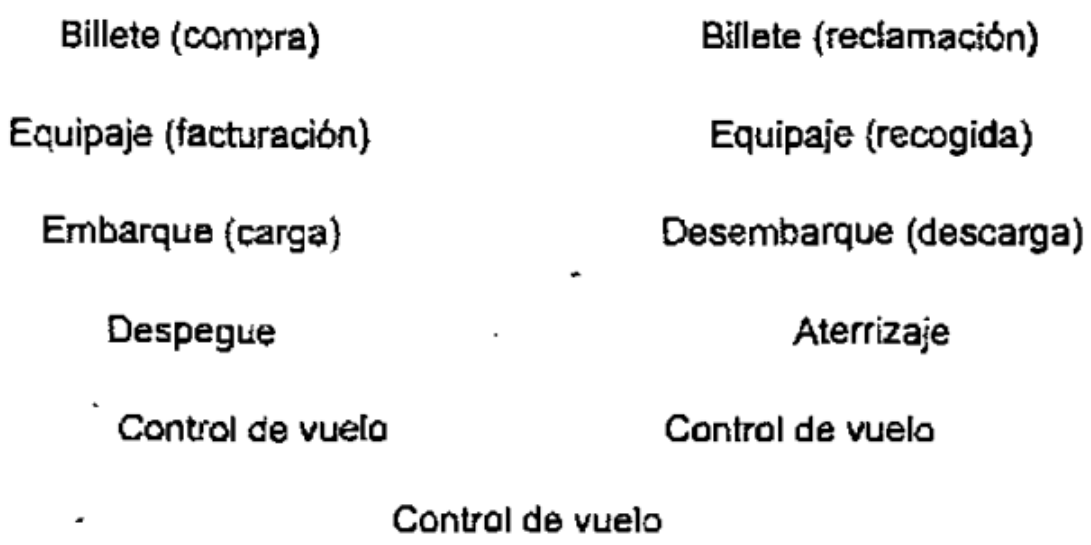

Figura 2.1. Pasos para realizar un vuelo en avión. Tomado de Redes de Computadoras: Un enfoque descendente basado en Internet (p.46) (5ª ed.), por Kurose, J. F. & Ross, K. W. 2010

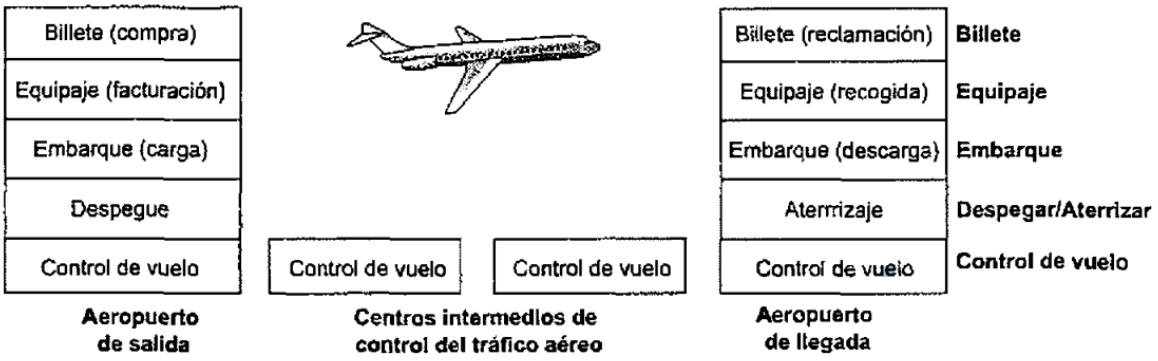

Figura 2.1.1. Ilustración de los pasos para realizar un vuelo en avión. Tomado de Redes de Computadoras: Un enfoque descendente basado en Internet (p.47) (5ª ed.), por Kurose, J. F. & Ross, K. W. 2010

En la siguiente imagen se muestran las capas organizadas en niveles en la parte izquierda de la figura y en la parte derecha encontramos el nombre correspondiente de cada capa de acuerdo con su nivel dentro del modelo.

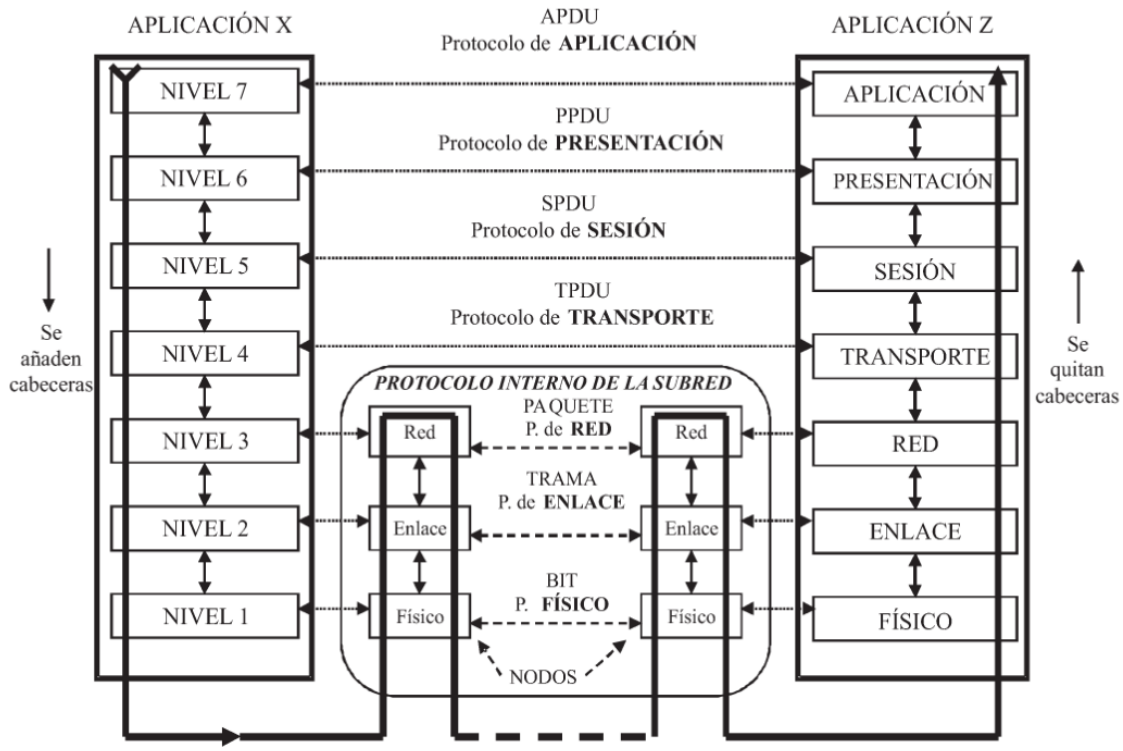

Figura 2.1.2. Ilustración las capas del Modelo OSI. Tomado de Redes de Computadores (p.23), por Sánchez Rubio, M. Barchino Plata, R. & Martínez Herráiz, J. J. (2020)

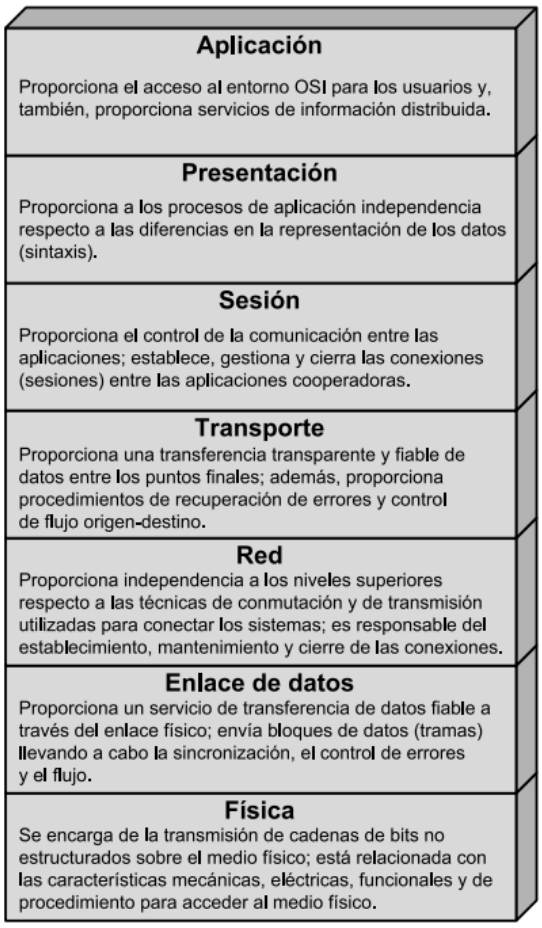

Figura 2.1.3. Capas del modelo OSI y breve definición. Tomado de Comunicaciones y Redes de Computadores (p.31) (7ª ed.), por Stallings, 2004

La imagen mostrada antes nos da una breve descripción de la función que tiene cada una de las capas dentro del Modelo OSI. Sabiendo como es que se encuentra conformado el Modelo OSI vamos a profundizar el que hace cada una de estas siete capas:

Capa Física

La capa física es la primera capa del Modelo OSI, esta es la responsable de transmitir los bits a través de un medio físico, como el cobre, aire o fibra óptica. Según Stallings (2014), esta capa crea y mantiene una conexión física entre los dos dispositivos que se están comunicando. Esta capa también se encarga de la codificación y decodificación de la señal en la transmisión, según. Según Stallings (2014), “la capa física se encarga de la representación de los bits en el medio físico y de las señales eléctricas, ópticas o electromagnéticas que representan esos bits” (p. 59).

La capa física tiene un papel importante en la gestión de errores en la transmisión, ya que cuando se están transmitiendo datos pueden ocurrir errores causados por

interferencias o perdida de señal. Esta capa posee mecanismos para detectar y corregir errores de transmisión. según Tanenbaum (2012), “la capa física se encarga de la detección y corrección de errores de transmisión mediante técnicas como la reducción de bits y la codificación de línea” (p. 87).

Para resumir, la capa física dentro del Modelo OSI es la encargada de transmitir los bits a través de medios físicos, gestionar los errores que se presenten y solucionarlos. Es muy importante y indispensable para que correcto funcionamiento de las capas superiores del modelo OSI.

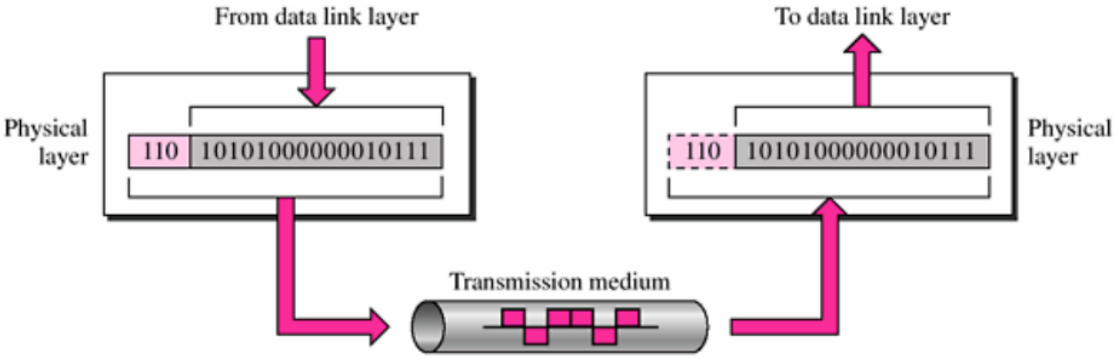

Figura 2.2 Representación de la Capa Física del Modelo OSI. Tomado de Comunicaciones y Redes de Computadores (7ª ed.), por Stallings, 2004

La imagen anterior representa el funcionamiento de la capa física, donde los bits se transmiten desde un origen a un destino mediante un medio de transmisión.

Capa de Enlace

La capa de enlace es la segunda capa del Modelo OSI, esta capa se “encarga de la transferencia de información entre entidades adyacentes en una red” (Tanenbaum, 2012, p.90). Busca proporcionar un servicio confiable y libre de errores a la capa de red, esto mediante métodos como detección y corrección de errores de transmisión. Según Stallings (2014), “esta capa se encarga de la transferencia de datos entre dispositivos adyacentes a través de un enlace de comunicación física, y proporciona los medios para la detectar y posiblemente corregir errores que puedan ocurrir en la capa física”.

Esta capa se encentra dividida en dos subcapas para garantizar su funcionamiento, estas capas son la LLC (Control de Enlace Lógico) y MAC (Control del Acceso al Medio). La primera subcapa la LLC es la que se encarga de gestionar la comunicación entre los diferentes dispositivos en una misma red, y la subcapa MAC es la que se encarga de asignar el medio de transmisión compartido, ya sea cable o mediante redes inalámbricas.

Forouzan (2012) afirma que, la capa de enlace realiza varias funciones clave, como encapsular datos, identificar el origen y destino de los datos, la detección y solución de errores y controlar el flujo de datos entre los dispositivos conectado y al mismo tiempo regular el acceso.

Para resumir, la capa de enlace es fundamental dentro del Modelo OSI para la transmisión de datos, garantizando confiabilidad entre los dispositivos de una red, esto ya que proporciona funciones como detectar y corregir errores, regular el flujo de los datos. De acuerdo con lo anterior, esta capa garantiza una comunicación fluida y libre de errores.

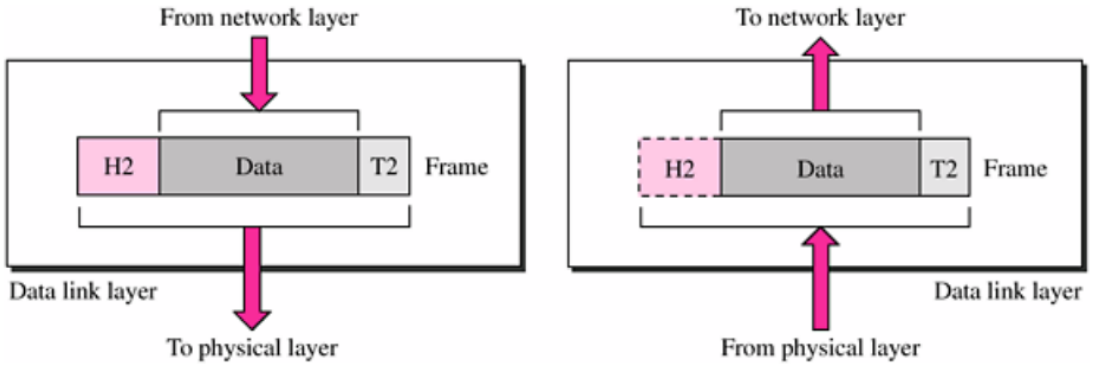

Figura 2.3 Representación de la Capa de Enlace del Modelo OSI. Tomado de Comunicaciones y Redes de Computadores (7ª ed.), por Stallings, 2004

La imagen presentada antes muestra la importancia de la capa de enlace con la capa de red y la capa física, dado que esta recibiendo información desde la capa de red y la transforma para que la capa física la envié a otro sitio donde nuevamente se transforma y vuelve a enviarse a la capa de red.

Capa de Red

La capa de red es la tercera capa del Modelo OSI, se encarga principalmente de la entrega de paquetes a través de diferentes redes. En esta capa se usa una dirección IP única para cada dispositivo conectado a la red y se encarga de enrutar los paquetes de manera eficiente para hacer que lleguen a su destino. Según Tanenbaum (2012), esta capa es la responsable de elegir la mejor ruta para enviar los datos en paquetes desde el origen hasta el destino.

Para el correcto funcionamiento de esta capa se utilizan direcciones lógicas que permiten identificar los dispositivos en la red y crear rutas entre estos. De acuerdo con Forouzan (2013), cada dispositivo en la red posee una dirección lógica única llamada IP (Protocolo de Internet), esta se usa por la capa de red para enrutar los paquetes de datos desde un origen hasta su destino.

Esta capa también se encarga de la fragmentación y reensamblado de los paquetes de datos para asegurar que se transmitan a través de las redes sin problemas. Esta capa divide los datos en paquetes y los envía a través de la red, y en el destino final la capa se encarga de reensamblar los paquetes para que los datos lleguen en su forma original.

Para resumir, la capa de red es esencial para la comunicación entre redes distintas y seleccionar la mejor ruta para enviar los datos hacia el destino, esto mediante el uso de direcciones IP y fragmentando y reensamblando los paquetes de datos.

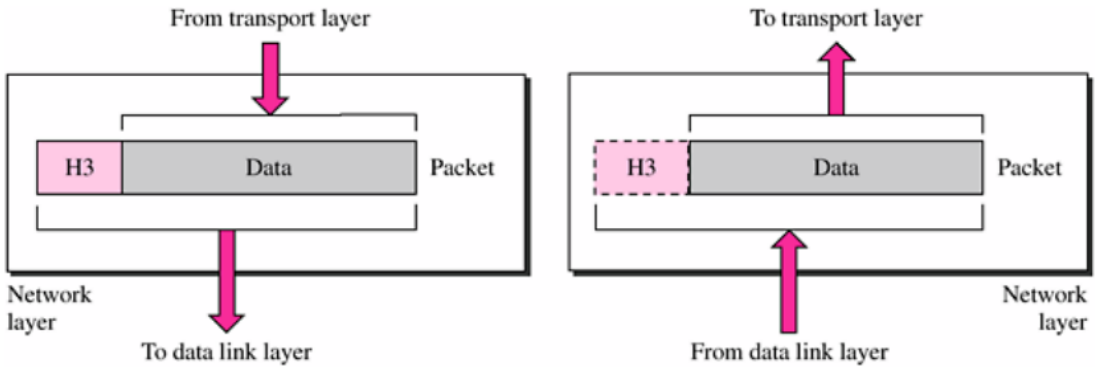

Figura 2.4 Representación de la Capa de Red del Modelo OSI. Tomado de Comunicaciones y Redes de Computadores (7ª ed.), por Stallings, 2004

La imagen presentada antes muestra la importancia de la capa de red con la capa de transporte y la capa de enlace.

Capa de Transporte

La capa de transporte es la cuarta capa del Modelo OSI, esta es la responsable de la entrega de datos de un extremo al otro extremo en un proceso de comunicación. Según Forouzan (2013), la capa de transporte "ofrece un control de flujo fiable, detección de errores y entrega secuencial de datos a través de la red" (p. 87).

En esta capa divide los datos en segmentos mas pequeños para que se puedan transmitir de manera mas eficiente y confiable. Además, posee mecanismos para detectar y corregir en la transmisión de los datos. Para esto la capa de transporte usa principalmente dos protocolos: TCP (Protocolo de Control de Transmisión) y UDP (Protocolo de Datagramas de Usuario).

El primer protocolo mencionado el TCP, es un protocolo enfocado a conexiones que establecen una conexión entre el origen y el destino antes de la transmisión de datos y garantiza que todos los datos se entreguen en orden y sin errores. El protocolo UDP, es un protocolo que funciona sin conexión que simplemente envía datos sin establecer una conexión previa, de este modo, no logra garantizar la entrega de los datos.

Resumiendo, la capa de transporte es esencial para garantizar la entrega de los datos de una manera eficiente entre un dispositivo de origen y uno de destino mediante el uso de distintos protocolos.

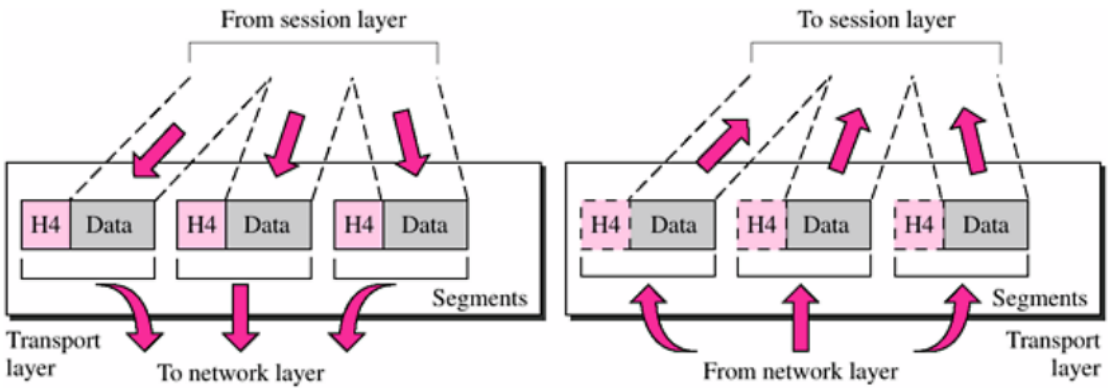

Figura 2.5 Representación de la Capa de Transporte del Modelo OSI. Tomado de Comunicaciones y Redes de Computadores (7ª ed.), por Stallings, 2004

Capa de Sesión

La capa de sesión es la quita capa del Modelo OSI, la principal función de esta capa es establecer, mantener y finalizar las conexiones entre aplicaciones de origen y destino. Es fundamental esta capa para garantizar que la comunicación entre las aplicaciones se pueda realizar de manera confiable.

Esta capa también es responsable de controlar la sesión de comunicación, lo que incluye la autenticación y autorización de los usuarios. Además, t9ene servicios para controlar errores, recuperación de fallas y retransmitir los datos en caso de que su transmisión se vea interrumpida.

Según Tanenbaum (2012), la capa de sesión puede proporcionar servicios de dialogo y sincronizado, lo que ayuda a que las aplicaciones se comuniquen en un determinado orden. Esta capa puede establecer puntos de control durante una sesión, esto permite que las aplicaciones retomen la comunicación en el punto en que se interrumpió.

Para resumir, la capa de sesión se encarga de un papel muy importante en la comunicación de redes, ya que establecer y mantiene conexiones seguras y confiables entre las aplicaciones. Además, proporciona servicios para la recuperación de errores y la retransmisión de datos en caso de fallas en la comunicación.

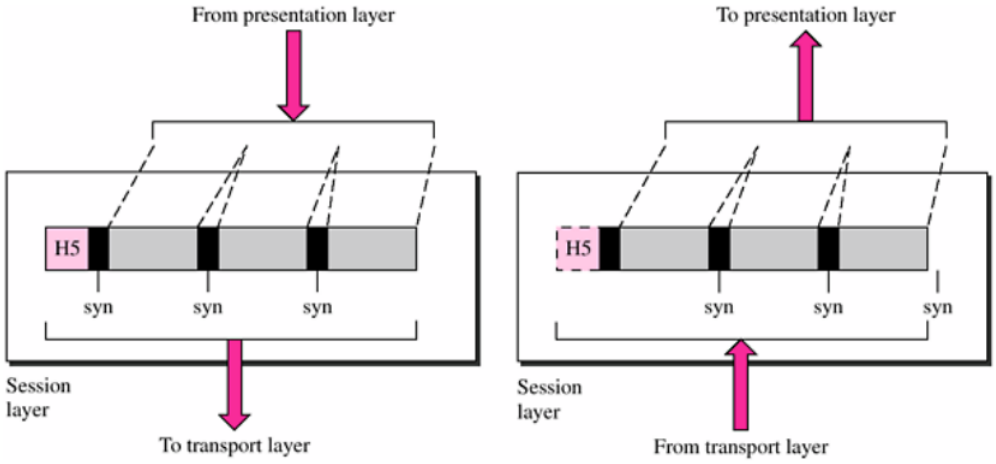

Figura 2.6 Representación de la Capa de Sesión del Modelo OSI. Tomado de Comunicaciones y Redes de Computadores (7ª ed.), por Stallings, 2004

Capa de Presentación

La capa de presentación es la sexta capa del Modelo OSI, esta capa se encarga de traducir los datos que se manejan en la capa de aplicación a un formato que pueda ser entendido por la diferentes aplicaciones y sistemas. También, se encarga de la compresión y el cifrado de datos. Según Tanenbaum (2012), la capa de presentación realiza principalmente tres funciones las cuales son "codificación de datos, compresión y cifrado".

Forouzan (2013), dice que la capa de presentación es la responsable de "asegurar que los datos que se reciben están en un formato que el destinatario pueda entender y procesar". Para ello esta capa utiliza diferentes formatos y protocolos, algunos de estos son JPEG para la compresión de imágenes y MPEG para la compresión de videos. También protocolos de cifrado como SSL y TLS, con los cuales puede asegurar la privacidad de datos durante las transmisiones.

Resumiendo, la capa de presentación es muy importante ya que es la que se encarga de garantizar la compatibilidad y seguridad de los datos transmitidos a través de una red, Además, de interpretar y comprimir los datos en diferentes formatos que garanticen que en el destino los datos puedan ser visualizados, todo lo anterior usando protocolos de cifrado que protegen los datos.

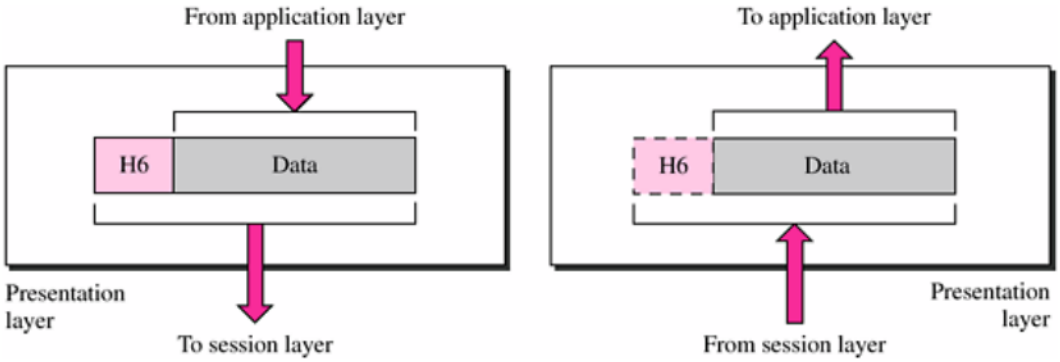

Figura 2.7 Representación de la Capa de Transporte del Modelo OSI. Tomado de Comunicaciones y Redes de Computadores (7ª ed.), por Stallings, 2004

La anterior imagen representa la capa de presentación del Modelo OSI, esta capa como todas las demás depende de las otras capas para permitir una correcta transmisión de los datos.

Capa de Aplicación

La capa de aplicación es la séptima y mas alta capa del Modelo OSI, esta es la que se encarga de proporcionar servicios de red a las aplicaciones con la que el usuario interactúa. Según Forouzan (2013), en esta capa el enfoque es principalmente a las necesidades de las aplicaciones y no en la forma en la que los datos se transmiten en la red.

Tanenbaum (2012), nos dice que en esta capa los protocolos que se usan son para aplicaciones del usuario, como lo es el correo electrónico, la transferencia de archivos, los accesos remotos a recursos de redes y entre otros. Esta capa también ofrece servicio se control de errores, autentificación y dialogo. Además, según Stallings (2013), Esta capa también es responsable de codificar y decodificar los datos en un formato para su transmisión en la red.

De manera resumida, la capa de aplicación es la capa mas alta de todo el Modelo OSI, esta es la capa de interfaz entre el usuario y la red, de este modo es responsable de proveer servicios de red a las aplicaciones del usuario. También, codifica y decodifica los datos en un formato común para su transmisión en la red.

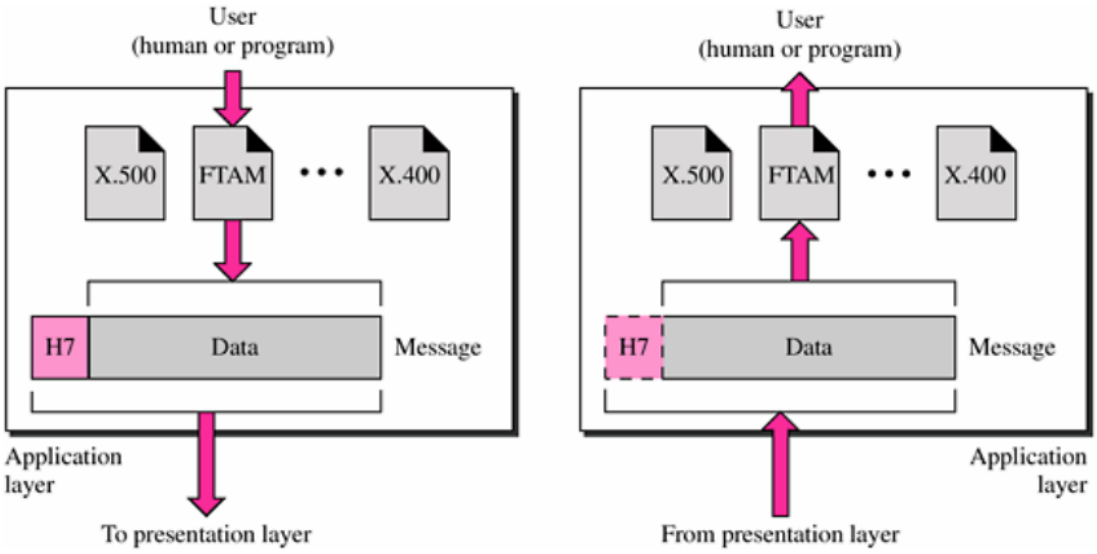

Figura 2.8 Representación de la Capa de Aplicación del Modelo OSI. Tomado de Comunicaciones y Redes de Computadores (7ª ed.), por Stallings, 2004

Protocolos por capa del Modelo OSI

Como se ha visto en el análisis de las capas del Modelo OSI, cada una de estas capas maneja distintivos protocolos que permiten la transmisión de los datos, la interoperabilidad, compatibilidad, seguridad, velocidad, entre otras características del modelo, por lo tanto, a continuación, vamos a profundizar un poco en los principales protocolos del Modelo OSI en sus capas.

Capa Física

En esta capa como se abordó anteriormente es la mas baja del modelo y se encarga de la transmisión de bits a través de medios físicos, por lo que los protocolos de esta capa buscan la transmisión de señales eléctricas o de luz. Los principales protocolos que encontramos en esta capa son:

- **RS-232:** Es un protocolo de datos serie, se usa principalmente para conectar dispositivos de comunicación de datos, estos dispositivos pueden ser módems y terminales a computadoras y otros equipos de redes. Este protocolo a sido usado ampliamente durante décadas en la industria de las comunicaciones, pero ha sido reemplazado por protocolos más modernos.
- **V.35:** Es un protocolo de comunicación de datos de alta velocidad que es utilizado para conectar dispositivos de red, como switches o routers a líneas de transmisión digitales y redes WAN.
- **Ethernet:** Es un protocolo de redes de área local que se utiliza para la transmisión de datos en redes de computadoras. Se usa para establecer una conexión entre dos dispositivos en una red y transmitir paquetes de datos entre

ellos. Este es uno de los protocolos más comunes usados en las redes y es compatible con una gran cantidad de dispositivos y sistemas operativos.

- **Token Ring:** Es un protocolo de redes LAN que define como los dispositivos se comunican entre sí en una red. Los dispositivos se conectan en un anillo y comparten un token para poder transmitir datos. Cuando un dispositivo tiene el token puede transmitir datos y los demás deben esperar a su turno para poder transmitir datos, actualmente este protocolo ha ido reemplazado por protocolos más modernos.
- **FDDI (Fiber Distributed Data Interface o Interfaz de datos distribuidos por fibra):** Es un protocolo de redes de área local de alta velocidad diseñado para transmitir datos a través de fibra óptica. se utiliza en aplicaciones que requieren alta velocidad, fiabilidad y seguridad, como en entornos de misión crítica en la industria financiera, aeroespacial y de defensa.
- **ATM (Asynchronous Transfer Mode O Modo de Transferencia Asíncrona):** Es un protocolo que se utiliza para transmitir información de manera eficiente en redes de alta velocidad, como las WAN y las LAN. Este protocolo divide los datos en pequeños paquetes llamados celdas, que se transmiten de manera asincrónica y se reensamblan en el destino, lo que genera una transmisión más rápida y eficiente d ellos datos.

Capa de Enlace

En esta capa se definen protocolos que permitan garantizar la entrega de datos confiable y sin errores a través de una red. Algunos de los protocolos mas comunes son los siguientes:

- **Ethernet:** Es un protocolo de redes de área local que se utiliza para la transmisión de datos en redes de computadoras. Se usa para establecer una conexión entre dos dispositivos en una red y transmitir paquetes de datos entre ellos. Este es uno de los protocolos más comunes usados en las redes y es compatible con una gran cantidad de dispositivos y sistemas operativos.
- **HDLC (High-Level Data Link Control o Control de enlace de datos de alto nivel):** Es un protocolo orientado a bit que proporciona una conexión de enlace de datos fiable entre dos dispositivos en una red. Es utilizado en una amplia variedad de redes, algunos ejemplos son las WAN, LAN y redes satelitales. En este protocolo los datos se dividen en tramas y se transmiten a través de un canal de comunicación, donde cada trama contiene un encabezado, un campo de datos y un tráiler. El encabezado y el tráiler de cada trama contienen información de control que se utiliza para gestionar la transmisión de datos.
- **PPP (Point-to-Point Protocol o Protocolo punto a punto):** Es un protocolo de comunicación de la capa de enlace de datos utilizado para establecer una conexión directa entre dos nodos de una red, este protocolo permite la transmisión de datos a través de diversas redes, incluyendo líneas telefónicas, cable módem, fibra óptica, satélite y conexiones inalámbricas.

- **Frame Relay:** Es un protocolo de comunicación de la capa de enlace de datos que se utiliza para conectar redes LAN y redes WAN mediante líneas de comunicación de alta velocidad como T1 o E1. Este protocolo transmite datos en paquetes llamados "tramas" a través de una conexión virtual permanente (PVC) o una conexión virtual conmutada (SVC) entre dispositivos de red. Estas tramas se transmiten a través de la red utilizando identificadores de conexión de enlace de datos (DLCI) que indican la dirección de destino de la trama. Es un protocolo eficiente y escalable que se utiliza en redes de gran tamaño y alta velocidad.
- **ATM (Asynchronous Transfer Mode O Modo de Transferencia Asíncrona):** Es un protocolo que se utiliza para transmitir información de manera eficiente en redes de alta velocidad, como las WAN y las LAN. Este protocolo divide los datos en pequeños paquetes llamados celdas, que se transmiten de manera asincrónica y se reensamblan en el destino, lo que genera una transmisión más rápida y eficiente d ellos datos.
- **Token Ring:** Es un protocolo de redes LAN que define como los dispositivos se comunican entre sí en una red. Los dispositivos se conectan en un anillo y comparten un token para poder transmitir datos. Cuando un dispositivo tiene el token puede transmitir datos y los demás deben esperar a su turno para poder transmitir datos, actualmente este protocolo ha ido reemplazado por protocolos más modernos.
- **FDDI (Fiber Distributed Data Interface o Interfaz de datos distribuidos por fibra):** Es un protocolo de redes de área local de alta velocidad diseñado para transmitir datos a través de fibra óptica. se utiliza en aplicaciones que requieren alta velocidad, fiabilidad y seguridad, como en entornos de misión crítica en la industria financiera, aeroespacial y de defensa.

Capa de Red

En esta capa se definen protocolos que permitan que los datos se entreguen desde una red a otra de una manera eficiente y confiable. Estos protocolos manejan el direccionamiento y enrutamiento de paquetes de datos, esto para asegurar que los datos sean enviados al destino correcto y en orden especifico. Algunos de los protocolos mas comunes de esta capa son:

- **IP (Internet Protocol o Protocolo de Internet):** Es el protocolo principal usado en el Internet, cumple la función de enrutar los paquetes de datos desde una fuente a un destino a través de una red. Es responsable de fragmentar y reensamblar los paquetes de datos si su tamaño es mayor al tamaño máximo que permite la red en la que se están transmitiendo. Este protocolo es usado por una gran variedad de otros protocolos para transmitir datos a través de Internet.
- **ICMP (Internet Control Message Protocol o Protocolo de mensajes de control de Internet):** Es un protocolo que se usa para él envió de mensajes de control y errores entre los dispositivos de una red. Es muy importante para un

correcto funcionamiento de las comunicaciones entre los aparatos de una red. Es usado por routers para informar de errores en la transmisión de paquetes, para realizar las pruebas de conectividad como el comando “ping”, y en otros diagnósticos de red.

- **ARP (Address Resolution Protocol o Protocolo de Resolución de Dirección):** Es un protocolo de red utilizado para mapear direcciones de capa de red (IP) a direcciones de capa de enlace (MAC). Su función es buscar en una red local la dirección MAC correspondiente a una dirección IP específica. Este protocolo es fundamental para el correcto funcionamiento de las comunicaciones en red.
- **RARP (Reverse Address Resolution Protocol o Protocolo de Resolución de Dirección Inversa):** Protocolo usado para obtener la dirección IP de una máquina cuando se conoce su dirección física (MAC). Este protocolo envía una dirección física y solicita su correspondiente dirección IP.
- **IGRP (Interior Gateway Routing Protocol Protocolo de Enrutamiento de Puerta de Enlace Interior):** Es un protocolo de enrutamiento interior utilizado en redes de área amplia (WAN) y en redes de área local (LAN) que utilizan el sistema operativo Cisco IOS. Lo que hace es calcular la mejor ruta para enviar paquetes de datos entre dispositivos de red.
- **OSPF (Open Shortest Path First):** Es un protocolo de enrutamiento de la capa de red que utiliza el algoritmo SPF (Shortest Path First) para determinar la mejor ruta de red entre dos nodos. Este protocolo es ampliamente utilizado en redes grandes y complejas, y es capaz de soportar redes de múltiples vías, lo que lo hace altamente escalable.
- BGP (Border Gateway Protocol o Protocolo de Puerta de Enlace Fronteriza): Es un protocolo de enrutamiento utilizado para intercambiar información de enrutamiento entre sistemas autónomos en Internet. Utiliza rutas y atributos de ruta para determinar la mejor ruta hacia un destino y es utilizado principalmente por proveedores de servicios de Internet y grandes redes empresariales que necesitan una conectividad confiable y escalable a Internet.
- **RIP (Routing Information Protocol o Protocolo de Información de Enrutamiento):** Es un protocolo de enrutamiento dinámico utilizado en redes de tamaño pequeño o mediano. Su función principal es el intercambio de información de enrutamiento entre routers vecinos para poder elegir la mejor ruta para enviar paquetes de datos a su destino.
- **IGMP (Internet Group Management Protocol o Protocolo de Gestión de Grupo de Internet):** Es un protocolo de comunicación utilizado por los hosts en una red IP para reportar su afiliación a uno o más grupos multicast. Permite que los dispositivos de red como routers y switches establezcan y mantengan los grupos multicast y controlen la transmisión de datos multicast en una red.

Capa de Transporte

En esta capa del Modelo OSI, la capa es responsable de la transmisión de datos confiable entre dos dispositivos finales. Algunos d ellos principales protocolos que usa esta capa son:

- **TCP (Transmission Control Protocol O Protocolo de Control de Transmisión):** Es un protocolo que se encarga de establecer una conexión fiable y orientada a la conexión entre dos dispositivos en una red, donde se asegura de que todos los paquetes de datos lleguen correctamente y en el orden correcto. Es utilizado comúnmente en Internet para la transferencia de archivos, correo electrónico, navegación web y otras aplicaciones que requieren una comunicación fiable y precisa.
- **UDP (User Datagram Protocol o Protocolo de datagramas de usuario**): Es un protocolo de la capa de transporte que proporciona un servicio de envío de datagramas sin conexión y no fiable. Es más rápido y ligero que TCP, pero no garantiza la entrega de paquetes ni verifica la integridad de estos. Se usa principalmente para aplicaciones en tiempo real que requieren una transmisión rápida de datos, como videojuegos, streaming de audio y vídeo, y VoIP.
- **SCTP (Stream Control Transmission Protocol o Protocolo de Control de Transmisión):** Es un protocolo de transporte utilizado en redes de comunicaciones para proporcionar una transferencia de datos fiable y orientada a la conexión entre sistemas finales. SCTP es similar a TCP en términos de fiabilidad, pero ofrece una mayor flexibilidad y soporte para aplicaciones que requieren múltiples flujos de datos simultáneos.
- **DCCP (Datagram Congestion Control Protocol o Protocolo de control de congestión de datagramas):** Es un protocolo de transporte que proporciona control de congestión para aplicaciones que utilizan datagramas de Internet, como VoIP (Voz sobre IP) y transmisión de medios en tiempo real.
- MPLS (Multiprotocol Label Switching o Cambio de Etiquetas Multiprotocolo): Es un protocolo de red que se utiliza para mejorar la eficiencia del enrutamiento de paquetes en redes de alta velocidad. MPLS asigna etiquetas a los paquetes de datos que identifican el camino que deben seguir a través de la red. De esta manera, se evita la necesidad de buscar la mejor ruta para cada paquete de forma individual, lo que agiliza el proceso de enrutamiento y reduce la carga en los routers de la red.

Capa de Sesión

En esta capa los protocolos se encargan de establecer, mantener y terminar sesiones entre dos aplicaciones que se están comunicando, también, sincronizan los datos, manejan un control de flujo y de errores en la comunicación. Algunos de los protocolos mas usados son:

- **RPC (Remote Procedure Call o Llamada a Procedimiento Remoto):** Es un protocolo que permite a un programa ejecutar una subrutina en un sistema remoto sin tener que entender los detalles de la comunicación de red.
- **NFS (Network File System o Sistema de Archivos de Red):** Es un protocolo que permite a los sistemas operativos compartir archivos y carpetas a través de la red.
- **X.225:** Es un protocolo de la capa de sesión utilizado para establecer conexiones entre dispositivos a través de una red.
- **ATP (AppleTalk Transaction Protocol):** Es un protocolo de capa de transporte utilizado para transmitir datos entre dispositivos en una red AppleTalk.
- **SIP (Session Initiation Protocol):** es un protocolo utilizado para establecer, modificar y finalizar sesiones de comunicación multimedia, como voz y video, en una red IP.
- **LDAP (Lightweight Directory Access Protocol):** Es un protocolo utilizado para acceder y modificar información almacenada en un directorio de red, como una base de datos de usuarios.
- **ASP (AppleTalk Session Protocol):** Es un protocolo utilizado para establecer y administrar sesiones de comunicación en una red AppleTalk.

Capa de Presentación

Esta es la capa del Modelo OSI que se encarga de la representación y el formato de los datos para asegurar que sean comprensibles por las aplicaciones de destino. Algunos de los principales protocolos de esta capa son:

- **JPEG:** Es un formato de compresión de imágenes digitales utilizado para reducir el tamaño de los archivos.
- **MPEG:** Es un formato de compresión de video y audio utilizado en la transmisión de televisión digital, DVD y otros medios.
- **ASCII:** Es un código de caracteres utilizado para representar texto en computadoras y otros dispositivos.
- **TIFF:** Es un formato de archivo de imagen utilizado para almacenar imágenes de alta resolución.
- **GIF:** Es un formato de imagen que admite animaciones y transparencias.
- **SSL/TLS:** Son protocolos de seguridad utilizados para cifrar las comunicaciones entre aplicaciones.
- **PDF:** Es un formato de archivo utilizado para representar documentos de manera independiente de la aplicación, el hardware y el sistema operativo.
- **HTML:** Es un lenguaje de marcado utilizado para crear páginas web.
- **XML:** Es un lenguaje de marcado utilizado para el intercambio de datos entre aplicaciones.
- **SNMP:** Es un protocolo utilizado para la gestión de redes y dispositivos.

Capa de Aplicación

En esta capa que se encarga de establecer la comunicación entre el usuario y las aplicaciones e intercambiar información entre estos dos. Los protocolos de esta capa incluyen funciones como transferencia de archivos, correos, navegación web y mensajería. Algunos de los principales protocolos de esta capa son:

- **HTTP (Protocolo de transferencia de hipertexto):** utilizado para transferir contenido web a través de la red.
- **FTP (Protocolo de transferencia de archivos):** utilizado para la transferencia de archivos a través de la red.
- **SMTP (Protocolo simple de transferencia de correo):** utilizado para la transferencia de correo electrónico.
- **POP3 (Protocolo de oficina de correos versión 3):** utilizado para la recepción de correo electrónico.
- **IMAP (Protocolo de acceso a mensajes de internet):** utilizado para la recepción y gestión de correo electrónico.
- **SNMP (Protocolo simple de gestión de red):** utilizado para la gestión y supervisión de dispositivos de red.
- **Telnet (Protocolo de red de terminal):** utilizado para la conexión y control remoto de dispositivos a través de la red.
- **DNS (Sistema de nombres de dominio):** utilizado para la resolución de nombres de dominio a direcciones IP.
- **DHCP (Protocolo de configuración dinámica de host):** utilizado para la asignación de direcciones IP y otra información de red a dispositivos.
- **SSH (Protocolo seguro de shell):** utilizado para la conexión y control remoto de dispositivos a través de una conexión segura.

Ventajas y desventajas

Como se ha mostrado anteriormente el Modelo OSI es una parte clave en el mundo de las redes de computadoras, ya que ofrece un estándar para la comunicación entre los dispositivos de diferentes plataformas o fabricantes. De este modo permite a desarrolladores y proveedores de equipos de red operar con un conjunto de estándares común que garantice la interoperabilidad y compatibilidad entre los diferentes dispositivos o tecnologías a emplear. Por lo tanto, encontramos que el Modelo OSI posee una serie de ventajas en su uso, pero también tiene sus desventajas que hacen que no sea un modelo perfecto, estas ventajas y desventajas se muestran a continuación:

Ventajas del Modelo OSI

Algunas de las principales ventajas que nos puede llegar a ofrecer el Modelo OSI son las siguientes:

- Proporciona una estructura mas clara y definida para las funciones de una red mediante la división en sus 7 capas: El modelo OSI nos ofrece una estructuración jerárquica

dividida en siete capas las cuales permiten separar las funciones de la red, esto permite que sea mucho más fácil la comprensión, modularidad y flexibilidad en el desarrollo de protocolos.
- Permite una interoperabilidad entre diferentes sistemas mediante el uso de estándares.
- Facilidad en el desarrollo e implementación de los protocolos de red mediante la división de funciones en capas.
- Permite una identificación y solución más eficiente y rápida de los problemas de red, ya que al estar dividida su funcionalidad en capas es más fácil encontrar en donde se está presentando el error.

Desventajas del Modelo OSI

Algunas de las principales desventajas que podemos identificar en el Modelo OSI son las siguientes:

- Es más complejo que el modelo TCP/IP: El modelo OSI es más complejo que el modelo TCP/IP porque tiene más capas y requiere más recursos para su implementación. Esto puede hacer que sea más difícil de entender y aplicar en entornos de red.
- No se utiliza ampliamente en la industria: A pesar de que el modelo OSI es un modelo bien fundamentado, no se utiliza ampliamente en la industria. Esto significa que puede ser difícil encontrar recursos, soporte y herramientas disponibles para su implementación y mantenimiento.
- Requiere una gran cantidad de recursos: El modelo OSI requiere una gran cantidad de recursos para su implementación, lo que puede ser una desventaja en entornos donde los recursos son limitados. Esto puede aumentar los costos y disminuir la eficiencia en la gestión de redes.
- Puede ser difícil de depurar y mantener: Debido a su complejidad, el modelo OSI puede ser difícil de depurar y mantener. Esto puede aumentar los costos de mantenimiento y reducir la eficiencia en la gestión de redes. En comparación con el modelo TCP/IP, que es más simple y práctico, el modelo OSI puede ser más difícil de depurar y mantener.

TCP/IP Model (Graphics, devices, protocols)

"TCP/IP is the glue that holds together the Internet and the World Wide Web."

Leiden, C., & Wilensky, M. (2009). TCP / IP For Dummies (6th ed.). John Wiley & Sons. P. 20

TCP/IP se define por los dos protocoles por los que se componen, el TCP, encargado del control de transmisión y el protocolo IP encargado del Internet, en este sentido TCP significa, en inglés, Transmission Control Protocol e IP significando Internet Protocol.

TCP/IP al ser el conjunto de protocolos que permiten la comunicación implementando la internet o bien en redes privadas cuenta con diferentes capas, cuatro en total, más sin embargo se puede definir como una capa extra, o “primer capa” la capa física (Cables, ondas de radio, etc.). Las otras cuatro capas son; Capa de acceso a la red, capa de internet, capa de transporte y la capa de aplicación, cada una de estas haciendo que TCP/IP pueda ser separado en estas y dividir las funciones y/o responsabilidades de la comunicación todo esto en diferentes niveles, simplificando el mantenimiento y funcionamiento total del protocolo, cada una de estas capas al trabajan independientes pero haciendo parte del todo, así que deben comunicarse una con otra para lograr la correcta transferencia de datos con eficiencia y fiabilidad.

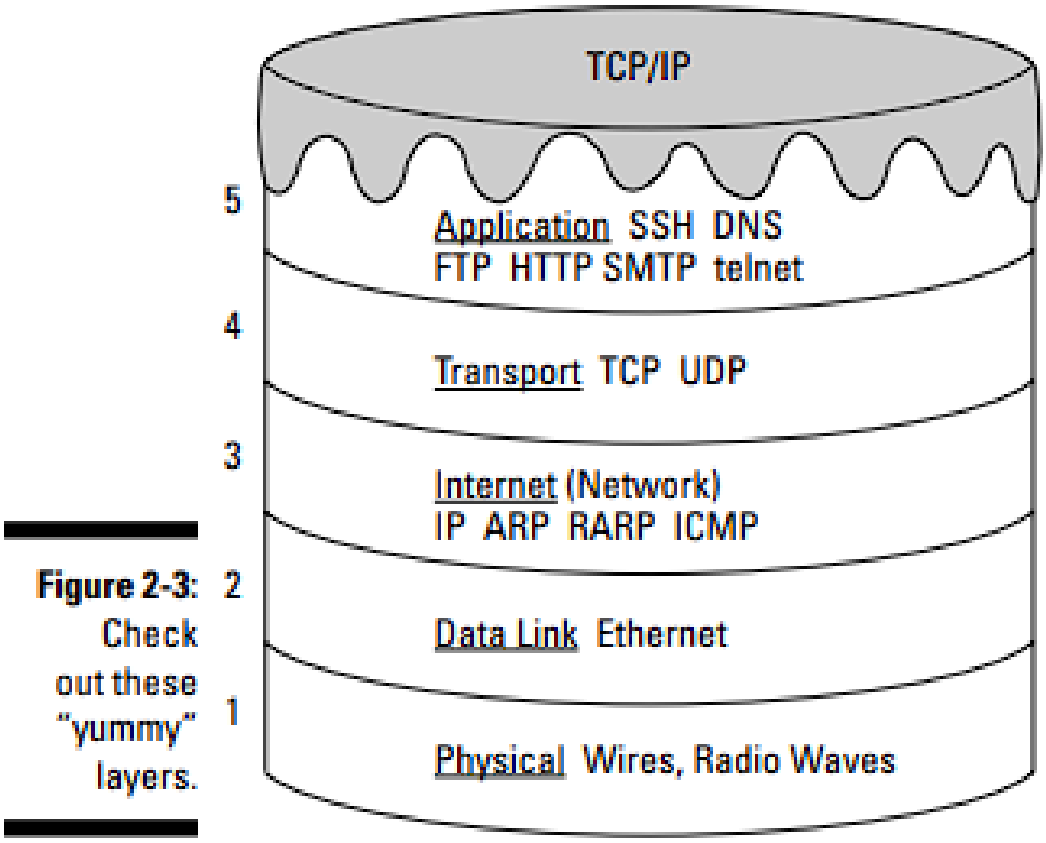

Figure 2-3: Check out these “yummy” layers.

Figura 3.1 Capas del protocolo TCP/IP

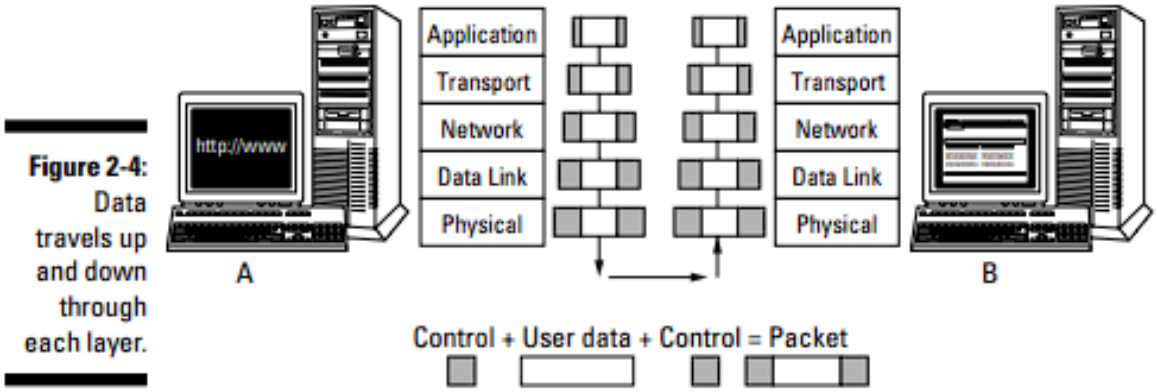

Figure 2-4: Data travels up and down through each layer.

Figura 3.2 Ejemplificación de las capas en la comunicación de dos computadoras

Como bien vemos en la figura 3.2, podemos ver cómo cada dispositivo, emisor y receptor tienen sus cinco capas, y vemos que al ser una pila se inicia desde la quinta capa hasta la primera para que el receptor reciba la señal transmitida y pueda volver a ser el mensaje enviado.

¡Por cierto! un protocolo como bien lo indica Leiden, C. & Wilensky, M. en el libro "TCP/IP for dummies" <<A protocol is a set of behavior-related rules that people follow. Some protocols are formally defined. For example, when people meet and greet each other, they might say, "How do you do">>. Es decir, un protocólo no es más que unas normas, reglas, pasos o estándares planteados e implementados por su funcionalidad, practicidad o porque simplemente, funciona correctamente y cumple su propósito, en este caso para TCP/IP conectar correctamente redes privadas o el internet en sí. Cabe resaltar que dichos protocolos son establecidos para que "el lenguaje" o la manera en la que se comunican los objetos, redes, etc. Sea efectiva, tal como los humanos nos comunicamos formalmente, siguiendo estándares, TCP/IP permite esta comunicación entre dispositivos.

"TCP/IP fits everywhere. Regardless of your geographical network technology, in the end it's TCP/IP that carries your data, such as e-mail or Web pages, to you." *Leiden, C., & Wilensky, M. (2009). TCP / IP For Dummies (6th ed.). John Wiley & Sons. P. 17*

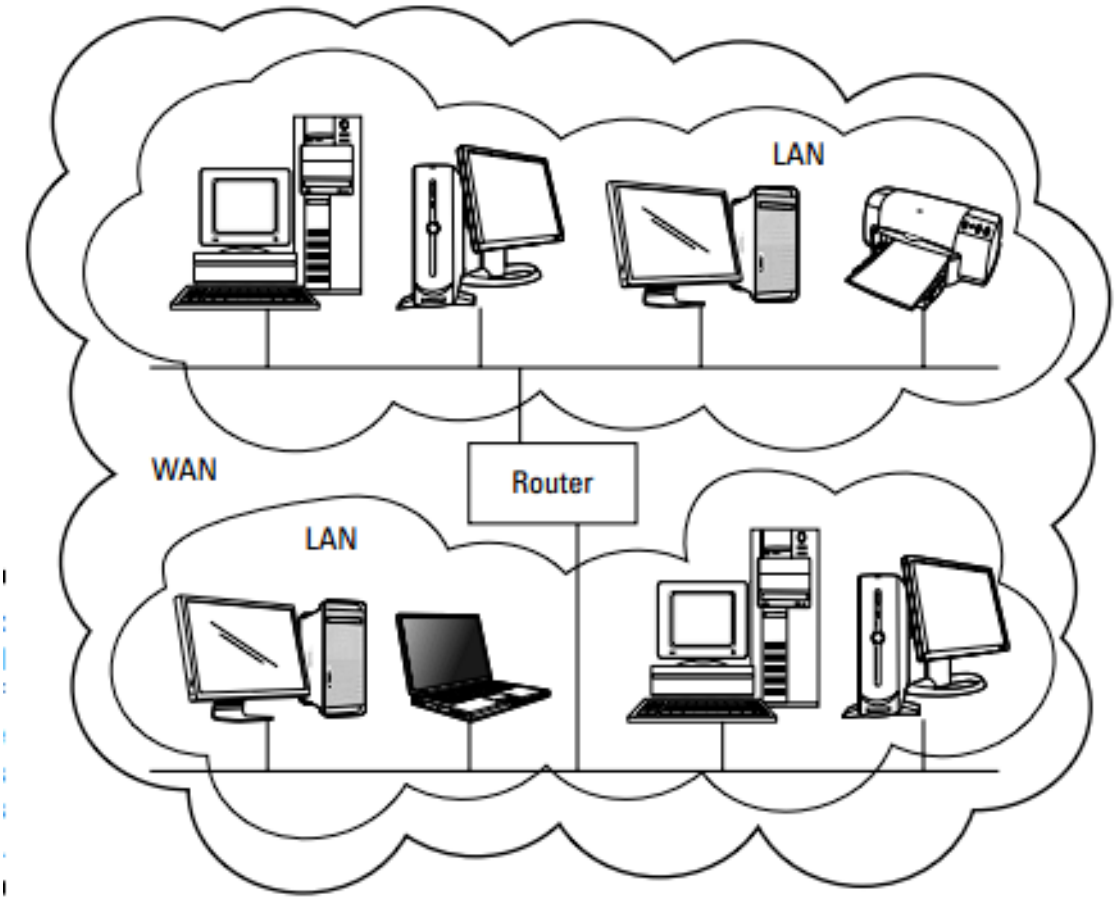

Figura 3.3 Dos redes LAN formando una red WAN.

Como bien lo indicamos anteriormente, y teniendo en cuenta el fragmento citado, el TCP/IP se encuentra en donde haya un mensaje que transmitir y que deba ser llevado de un extremo a otro, en la figura anterior vemos como hay red WAN dividida en dos redes LAN, en este caso el protocolo TCP/IP permitirá que ambas redes LAN puedan enviar y recibir mensajes, señales o transmisiones. Resaltemos también que no tiene sentido tener "Software" si no hay un "Hardware" que permita utilizarlo, en este caso las redes, LAN, WAN, MAN, etc. Son el hardware que permite que el protocolo TCP/IP tenga sentido y pueda ser implementado.

Antes de hablar sobre cada una de las capas hay que tener en cuenta que el protocolo TCP/IP transforma todos lso mensajes que deseamos transmitir en paquetes, pequeños bites y los envía a través de la red y cuando los paquetes llegan a su destino, TCP/IP se encarga de rearmar los paquetes, desempaquetarlos y devolverlos al mensaje original.

- **Capa física:**

En este caso podemos hablar de una capa que se define como la parte física en el sentido de que se hace referencia al hardware, todo aquello que permite la transmisión de señales, los medios de transmisión sean guiados o no guiados, además de también hablar de componentes importantes para el modelo como lo es el NIC, repetidores, modems, etc. que permite que los dispositivos puedan conectarse a la internet. Esta capa es en donde cada una de las señales electricas son transmitidas, y como bien mencionamos al ser la parte física aquí es donde la data es transformada en bits que serán transmitidos como señales.

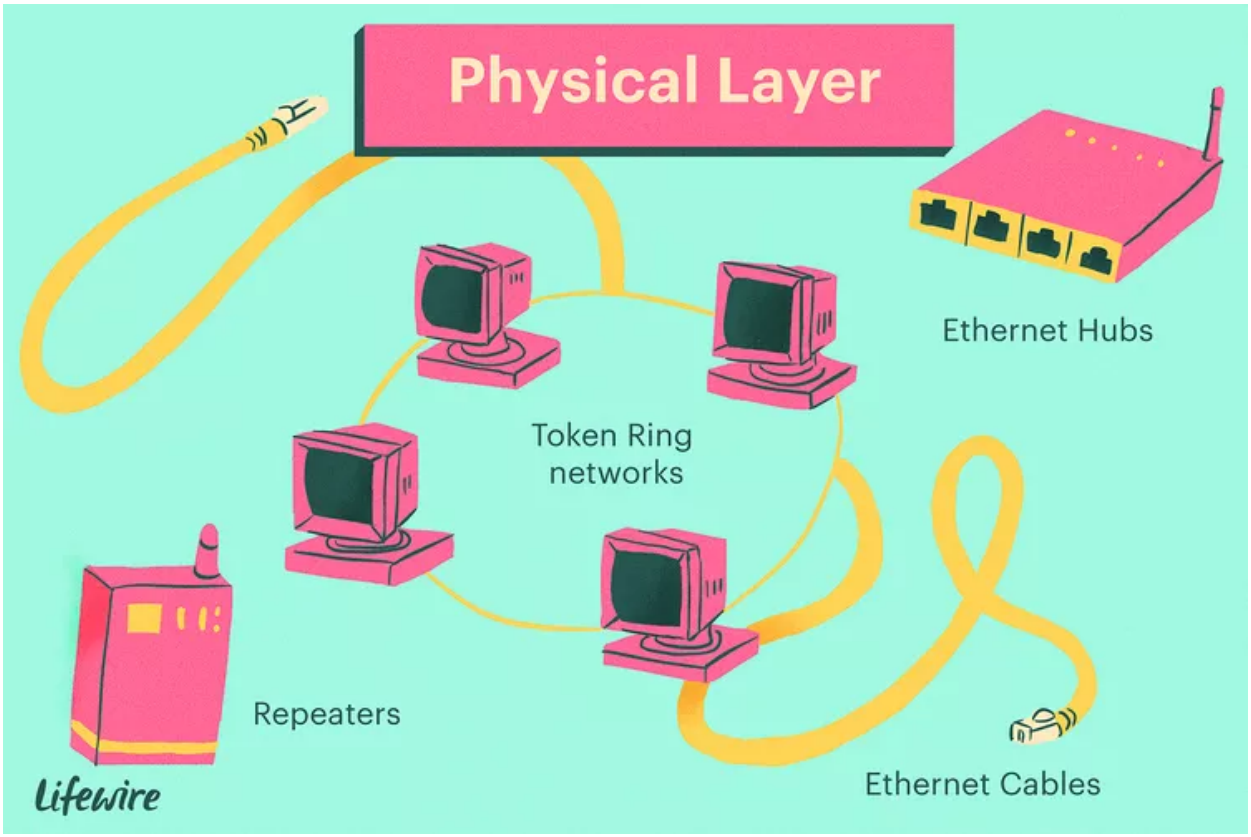

Figura 3.4 Tomado de https://www.lifewire.com/layers-of-the-osi-model-illustrated-818017

- **Capa de acceso a la red:**

En la capa de Acceso a la red, se encarga de la transmisión de los paquetes de datos a través de la red, dividiéndolos en fragmentos para su envío por el medio de transmisión correspondiente, ya sea guiado o no guiado. Esta capa también se encarga de enrutar los paquetes de datos a su destino, utilizando protocolos de direccionamiento y enrutamiento IP. Además, en esta capa se realizan las conexiones a las redes privadas virtuales (VPN) y se permite el envío de los paquetes de datos a la dirección MAC correspondiente gracias a los protocolos de dirección o conexión NIC. Asimismo, esta capa se encarga de gestionar la

interferencia en la transmisión de los datos para evitar pérdidas de información en las señales transmitidas.

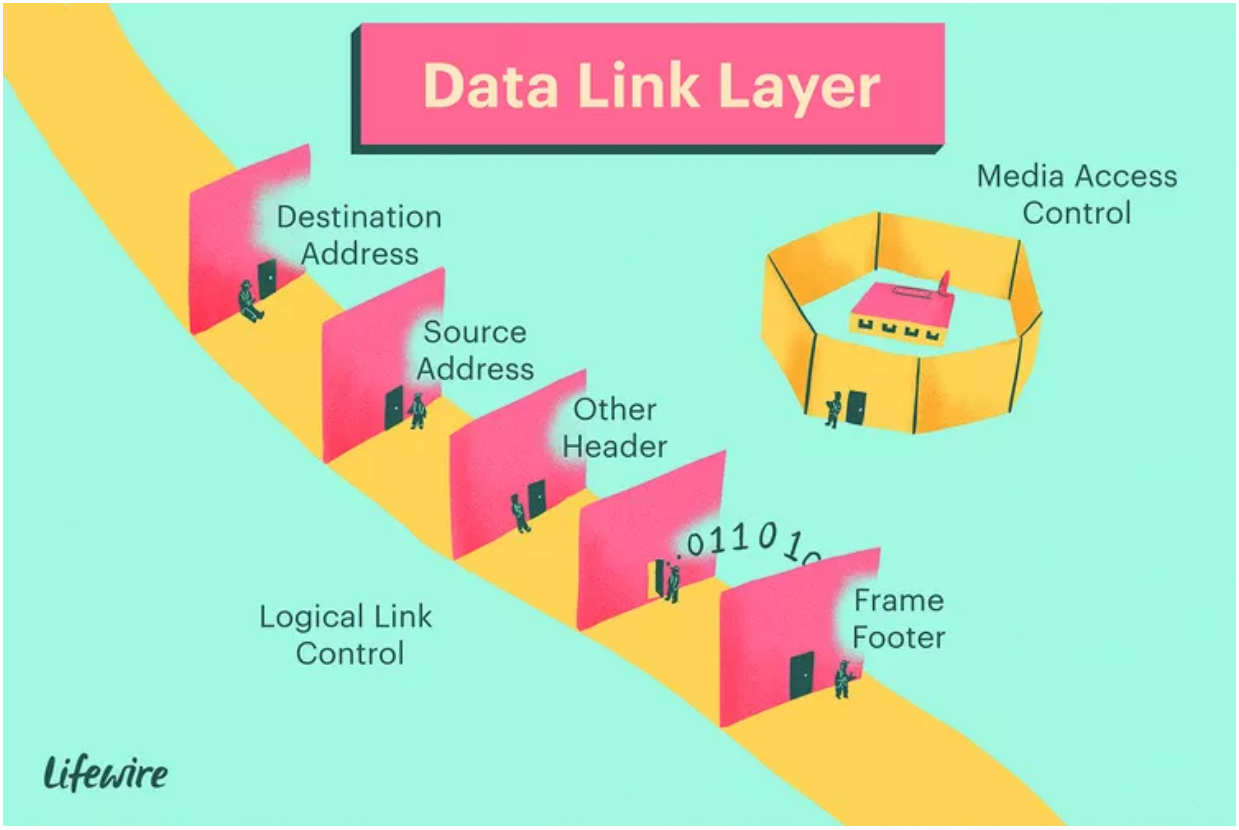

Figura 3.5 Tomado de https://www.lifewire.com/layers-of-the-osi-model-illustrated-818017

- **Capa de internet:**

Esta capa es la primera en la que hablamos de software, y en la cual por consiguiente ya encaja y empieza a aplicarse el protocolo TCP/IP a la transmisión de las señales, en este caso a través de la IP, en esta capa se reciben los paquetes de la capa dos, la de acceso a la red y todos estos paquetes son enviados a la dirección correcta, en este caso como bien entendemos por la dirección IP. Si en dado caso hay más de una posible ruta o de dirección, la capa se encarga de escoger la ruta más adecuada o la mejor para que reciba la transmisión, pensémoslo como si compramos un producto por internet y nuestra dirección coincide con otra, el correo/transportadora (la capa) se encargará de validar a cuál será enviado el paquete y escogerá la mejor vía. Sin esta capa simplemento sería imposible que la información pudiese llegar al lugar correcto, a la dirección establecida por el emisor.

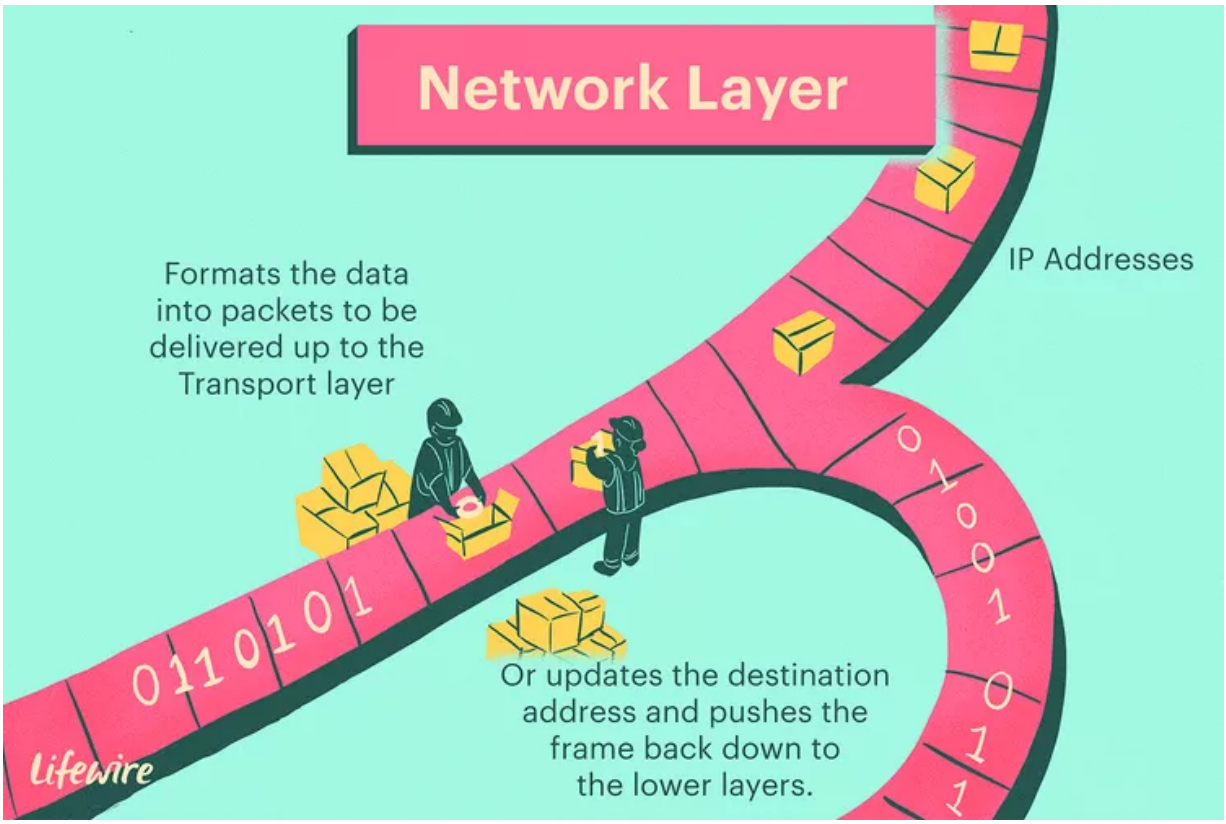

Figura 3.6 Tomado de https://www.lifewire.com/layers-of-the-osi-model-illustrated-818017

- **Capa de transporte**

Como vimos en la capa anterior, esta es la encargada de enviar los paquetes a la dirección correcta así transmitiendo correctamente. Siendo así debemos tener en cuenta lo que definimos al inicio sobre TCP/IP y que entendemos que las capas existen para que la transmisión sea dividida y el trabajo igual, dada la situación la capa de transporte recibe la dirección que la capa anterior encuentra y en esta capa se realiza el correcto envío de los paquetes para que la información no tenga ruido, se disperse y así las señales lleguen correctamente y sin perder data en el transporte y que cada uno de los paquetes enviados lleguen a su destino, retomando el ejemplo de la capa anterior, en esta capa (de transporte) es el repartidor que recibe la información del correo y debe repartir, hacer llegar y en el orden correcto, todos los paquetes.

En esta capa se utilizan dos protocolos el TCP (transmission Control Protocol) y el UDP (User Datagram Protocol), que bien definidos podemos decir que el UDP es un protocolo que no proporciona garantías para la entrega de los datos, por esto mismo es más rápido y eficiente que el protocolo TCP que podemos definirlo como un protocolo orientado a la garantía de que todos los paquetes sean entregados como lo mencionamos en el párrafo anterior, pero contrastando con el UDP se pierde eficiencia y velocidad.

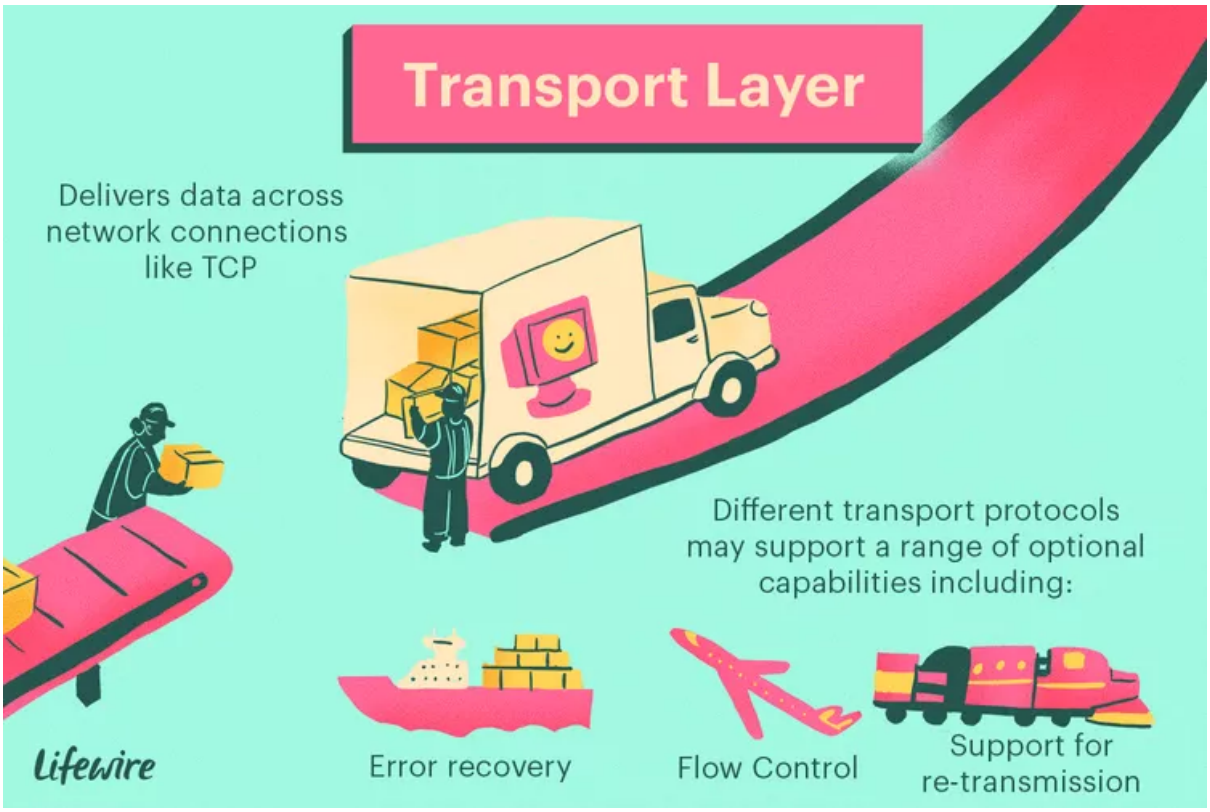

Figura 3.7 Tomado de https://www.lifewire.com/layers-of-the-osi-model-illustrated-818017

- **Capa de aplicación:**

En esta capa podemos definir que se realiza el desempaque, valga la redundancia, de los paquetes que fueron enviados y transportados hasta la dirección correcta, haciendo que las señales y toda la información vuelva a su estado original, y el receptor reciba lo que se envió. En esta capa se hace uso de protocolos de red tales como HTTP, FTP; SMTP entre otros, y la presentación de los datos se realiza en un formato legible por el recepto, y en esta capa se pueden implementar servicios de seguridad, autenticación, encriptación etc. Y así proteger la comunicación entre las aplicaciones de la capa.

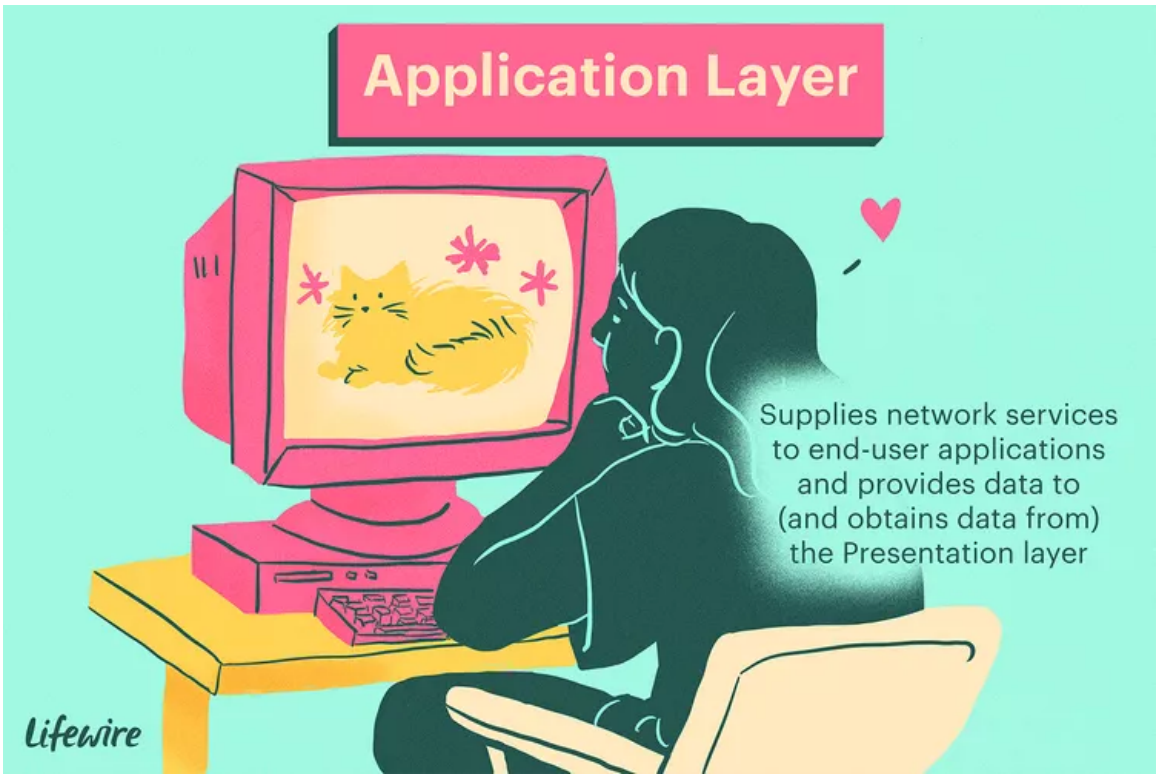

Figura 3.7 Tomado de https://www.lifewire.com/layers-of-the-osi-model-illustrated-818017

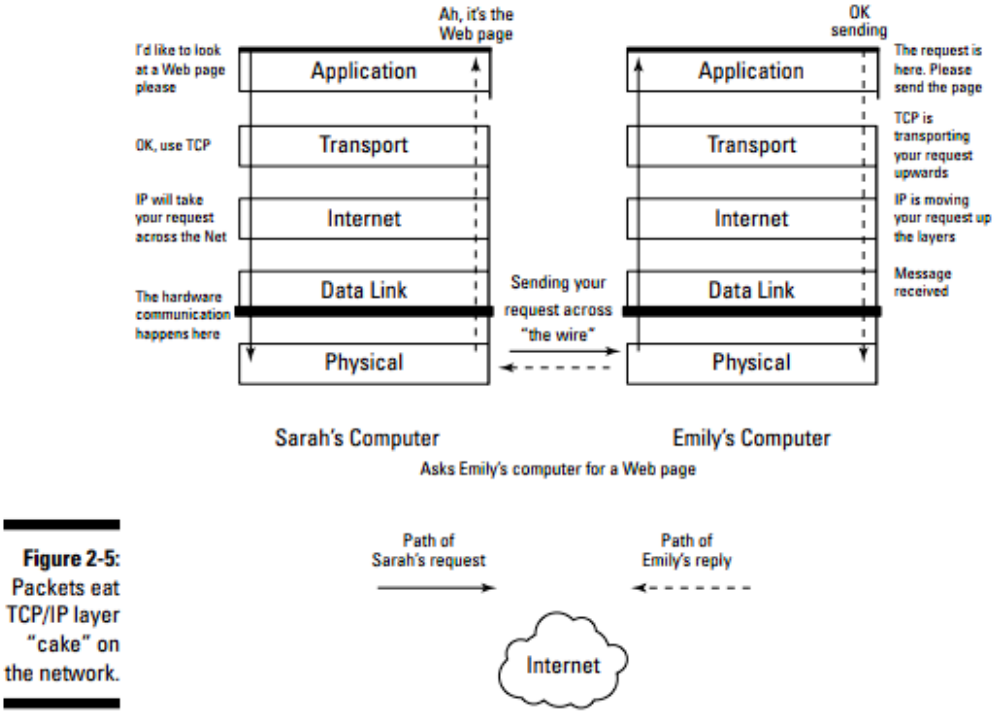

Figure 2-5: Packets eat TCP/IP layer "cake" on the network.

Figura 3.8 El funcionamiento de las capas en una comunicación entre dos computadores.

Como vemos en la figura 3.8 Sarah le solicita al computador de Emily por una página web, y en cada una de las capas vemos cómo funciona como lo definimos con anterioridad y cómo se comunican ambos computadores para que la solicitud de Sarah sea respondida por Emily así proporcionándole la página web deseada. Todo este proceso no habría sido posible, y Sarah no se habría podido comunicar con Emily sin el protocolo TCP/IP.

- **Protocolos de la capa de internet:**
  - IP: Internet Protocol

En este apartado, es importante destacar que el protocolo IP es esencial en la arquitectura TCP/IP, ya que sin él, el protocolo TCP no podría enviar los paquetes a su destino, lo que haría que todo el sistema carezca de sentido.

El protocolo IP se encarga de asignar una dirección única a cada dispositivo conectado a Internet, lo que permite a la capa de transporte encontrar la dirección correcta para llevar los paquetes donde deben ir. Además, este protocolo funciona sin establecer una conexión previa, lo que significa que la definición de las direcciones y los paquetes que serán enviados se realiza de manera individual, sin necesidad de generar una conexión previa para determinar la dirección de destino de los paquetes.

El protocolo IP se encarga de asignar una dirección única a cada dispositivo conectado a Internet, lo que permite a la capa de transporte encontrar la dirección correcta para llevar los paquetes donde deben ir. Además, este protocolo funciona sin establecer una conexión previa, lo que significa que la definición de las direcciones y los paquetes que serán enviados se realiza de manera individual, sin necesidad de generar una conexión previa para determinar la dirección de destino de los paquetes.

  - IPv6: Internet Protocol version 6

  - ARP: Address Resolution Protocol

El protocolo de resolución de direcciones, ARP, nos permite en la capa de internet poder encontrar la dirección MAC de dispositivos a partir de su dirección IP. Es útil cuando una computadora necesita comunicarse con otra en la misma red, de esta manera se obtiene la dirección MAC que es más precisa en la manera de identificar un dispositivo de una misma red. El funcionamiento de ARP es sencillo, la computadora o dispositivo que

necesita enviar información a otra computadora de la cual desconoce su dirección MAC, hace una solicitud a todos los dispositivos de la red con la dirección IP del dispositivo que se desea y sólo este responderá con su dirección MAC, así el dispositivo emisor sabrá a dónde enviar los paquetes e información.

- RARP: Reverse Address Resolution Protocol

"When a computer knows only its own MAC address, the Reverse Address Resolution Protocol (RARP) lets it find out the IP" *Leiden, C., & Wilensky, M. (2009). TCP / IP For Dummies (6th ed.). John Wiley & Sons. P. 30*

Este protocolo, en español Protocolo de Resolución INversa de Direcciones, como bien lo indica su nombre es el contrario de ARP ya que este lo que hace es encontrar la dirección IP a partir de la dirección MAC. Cabe aclarar que este protocolo prácticamente no sigue siendo usado porque los dispositivos cuentan con dirección IP establecida y no es definida al iniciar el dispositivo, como anteriormente, y por lo cual se creo este protocolo. De la misma forma que en el protocolo Arp, definido anteriormente, el dispositivo que desea obtener la dirección IP de otro dispositivo, hace broadcast compartiendo la dirección MAC y el dispositivo que coincida con esta, compartirá su dirección IP para así el dispositivo emisor saber a cuál dirección podrá enviar la información.

- ICMP: Internet Control Message Protocol

El protocolo ICMP, como bien lo utilizamos en Cisco Packet Tracer, y como lo vemos desde allí, se encarga de validar si una red y la conexión entre dispositivos está correctamente y funciona. Este protocolo nos devolverá o indicará si ocurre algún problema en el envío de los paquetes y si no es posible que llegue hasta el receptor e indicarle al emisor esto. Es importante para el protocolo TCP/IP ya que permite que cada uno de los dispositivos se puedan comunicar entre ellos y así validar correctamente que el envío y recepción de información funciona correctamente.

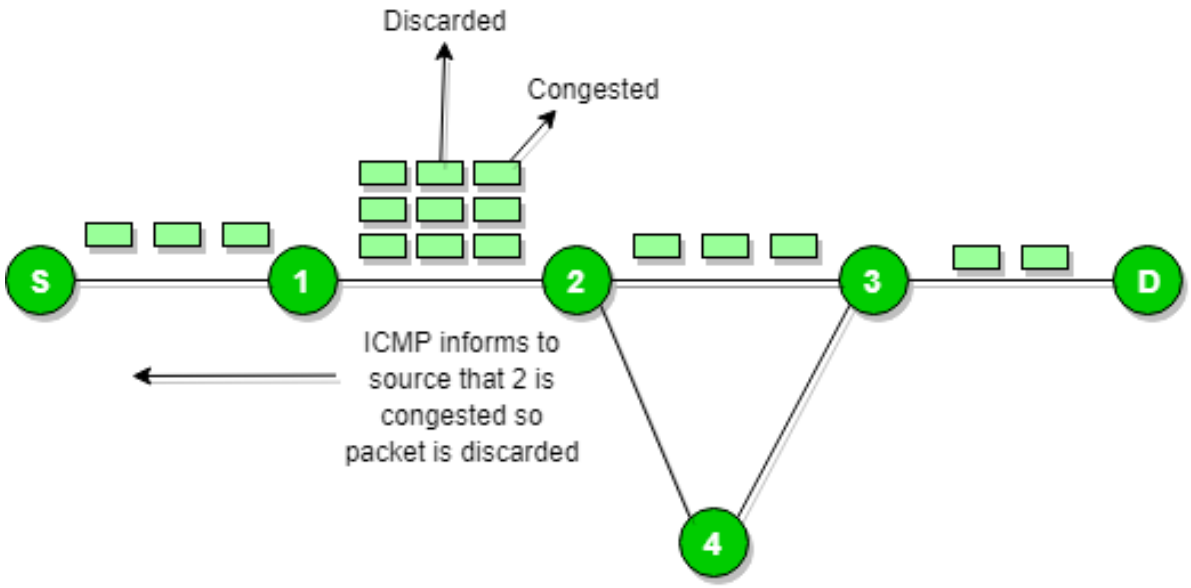

Figura 3.9 tomada de https://www.geeksforgeeks.org/internet-control-message-protocol-icmp/

- Mobile IP

El protocolo IP funciona perfectamente para dispositivos estáticos tales como lo pueden ser las impresoras, computadoras etc. Más sin embargo debemos tener en cuenta que existen dispositivos móviles como los teléfonos que van cambiando de red constantemente, siguiendo esto podemos creer que en cada red debe haber un cambio de IP para el dispositivo, siendo así cada dispositivo debe que pedir constantemente la dirección Ip del dispositivo, pero para solucionar esto existe el protocolo Mobile IP, este mismo permite que los dispositivos como los teléfonos puedan tener direcciones IP permanentes, conocida como "Dirección de inicio", permitiendo que el dispositivo tenga una conexión estable.

- IPSec: IP Security Protocols

Este protocolo es la parte que permite que la transmision de datos sea segura, y es utilizado principalmente para asegurar la privacidad y autenticidad de la información precisamente en redes de datos públicas. Este protocolo cuenta con dos subprotocolos, uno que encapsula la información ESP, y otro que permite hacer la autenticación de esta información AH, ambos al ser subprotocolos de uno principal, trabajan para poder brindar servicios de seguridad tales como autenticación de extremo a extremo de la comunicación, confidencialidad de datos, la integridad de los mismos y una protección contra ataques DDOS, o ataques de repetición. Este protocolo es permitido entre dos dispositivos cuando entre ellos se establezca una conexión segura y el protocolo pueda hacer su trabajo entre la transmisión de datos entre los dispositivos.

- L2TP: Layer 2 Tunneling Protocol

En el sentido de TCP/IP, L2TP es un protocolo de túnel que opera en, se utiliza para crear conexiones VPN seguras a través de redes públicas como Internet. Este protocolo establece un túnel entre dos puntos finales, de extremo a extremo, para establecer la conexión y autenticar a los usuarios que disponen de los dispositivos conectados. Una vez establecida la conexión, los paquetes de datos son encapsulados en un formato específico y enviados a través del túnel creado por el protocolo y por los dispositivos. L2TP es comúnmente utilizado en soluciones VPN y se ha convertido en un estándar de facto para la creación de túneles de red seguros. L2TP a menudo reemplaza al protocolo de túnel punto a punto (PPTP), un protocolo de cifrado más antiguo, y utiliza IPSec para cifrar los mensajes que se mueven a través de los túneles de VPN.

- CIDR: Classless Inter-Domain Routing

Finalizando los protocolos de la capa de internet, tenemos el protocolo CIDR (Classless Inter-Domain Routing), este es un método utilizado en Internet para asignar y gestionar direcciones IP de una manera más eficiente. Este método reemplaza el enrutamiento basado en clases con bloques de direcciones IP variables para permitir una mayor flexibilidad en la asignación de direcciones. Además, CIDR se utiliza para definir subredes en redes IP, lo que permite una asignación de direcciones más precisa y eficiente. CIDR también ayuda en el enrutamiento de paquetes y ha permitido la conservación de direcciones IP en un momento en que se temía que Internet se quedara sin direcciones disponibles.

- **Protocolos de la capa de transporte:**
  - TCP: Transmission Control Protocol

Como bien tenemos definido, el protocolo IP es quien indica las direcciones a donde debe ser enviados los paquetes, pero no es desde este protocolo que se realiza el envío, en este sentido podemos definir el protocolo TCP como el repartidor, el que toma la dirección IP y es quien va hasta allí y reparte los paquetes en el orden estimado y de la manera correcta, sin perder ni un sólo paquete. Tcp asegura y garantiza que todos los paquetes lleguen como se entregaron, y en el orden correcto como bien lo mencionamos anteriormente. Además actúa como una red de seguridad asegurando que las aplicaciones en la capa superior reciban los datos correctos.

En este protocolo, TCP se encarga de enumerar cada paquete de manera secuencial y en el orden que debe además de chequear y asegurarse de que no haya ningún error con los paquetes.

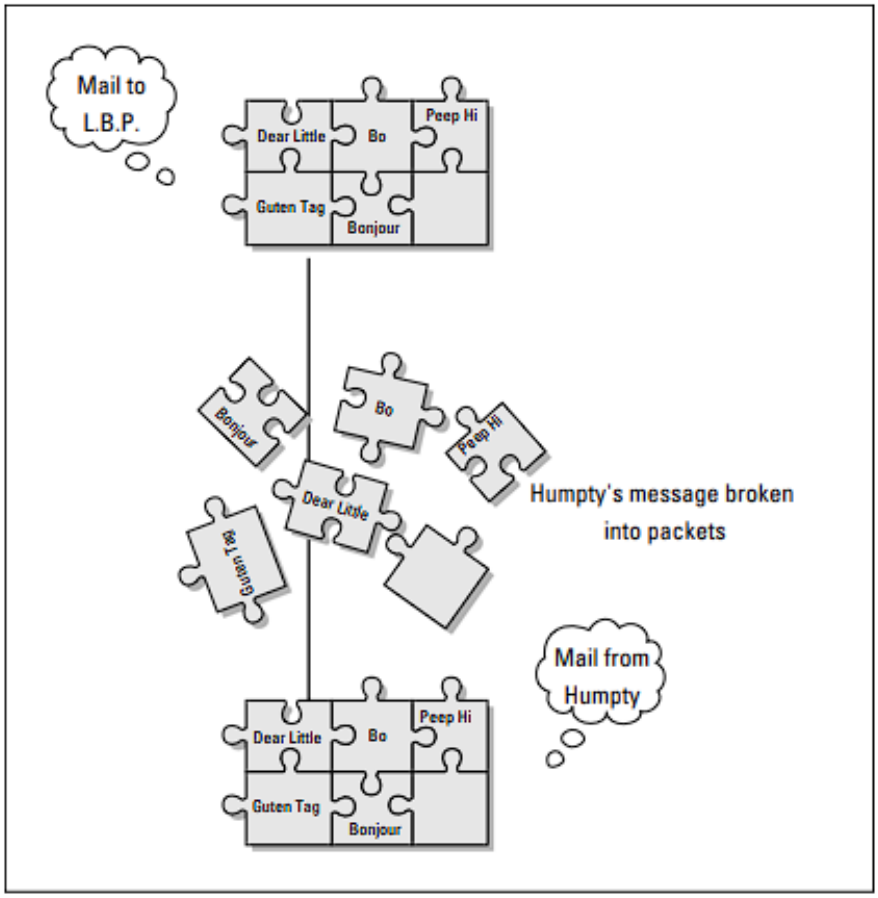

Figure 2-6: TCP sequences packets correctly.

Figura 3.9 TCP actuando y cumpliendo su trabajo

- UDP: User Datagram Protocol

UDP (User Datagram Protocol) es un protocolo sin conexión que funciona enviando paquetes, llamados datagramas a una dirección IP específica, tal como lo hace el protocolo TCP indicado anteriormente. UDP no garantiza la entrega de paquetes ni que éstos lleguen en el orden correcto a diferencia del protocolo TCP que sí realiza la enumeración y validación de cada paquete para que llegue a conformidad, perdiendo eficiencia y velocidad, en este aspecto el protocolo UDP es superior. A pesar de ser menos fiable que TCP, UDP transporta de forma segura una cantidad significativa de datos a través de la red y permite el flujo de datos entre los dispositivos.

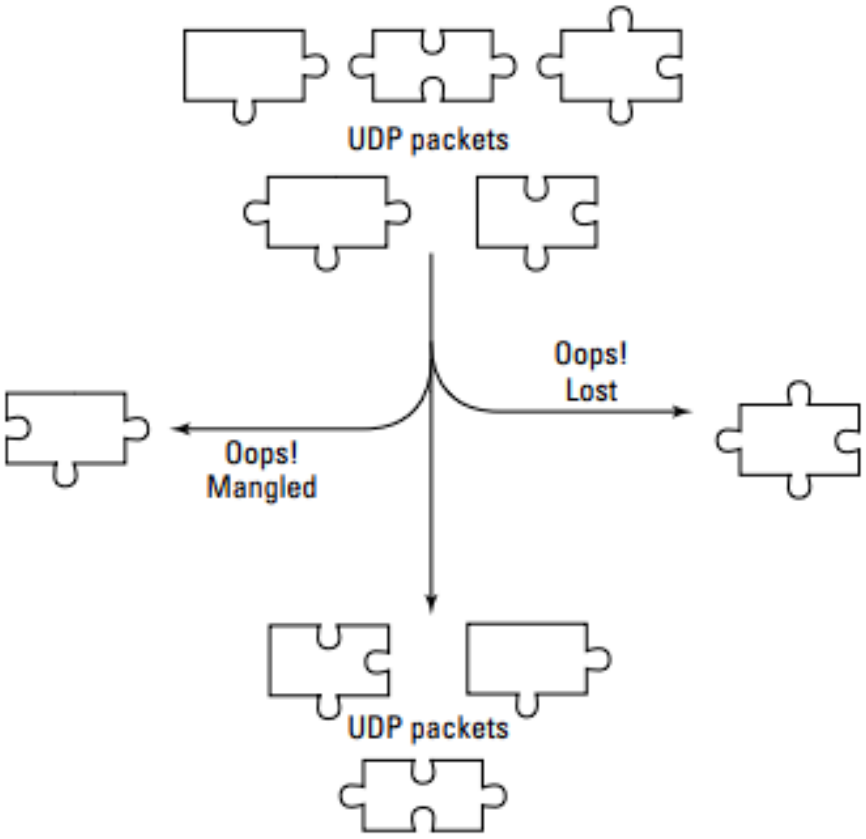

Figure 2-7: UDP might drop packets.

Figura 3.10 UDP diagram

- Routing protocols: Interior and exterior

Los protocolos de enrutamiento son esenciales en las redes informáticas, ya que permiten que los dispositivos de red se comuniquen entre sí y encuentren la mejor ruta para enviar datos. Hay dos tipos de protocolos de enrutamiento en el protocolo TCP/IP: Interior y Exterior. Los protocolos de enrutamiento interior son utilizados dentro de una red, como routers que utilizan el protocolo RIP, OSPF o EIGRP. Mientras que los protocolos de enrutamiento exterior son utilizados para conectar diferentes redes entre sí, como BGP. Los protocolos de enrutamiento exterior permiten que los routers intercambien información con otros routers fuera de su red local y tomen decisiones sobre la mejor ruta para enviar datos a través de múltiples redes.

- TLS: Transport Layer Security

TLS (Transport Layer Security) es un protocolo de seguridad que se utiliza para garantizar la privacidad y la integridad de la información que se transmite a través de

Internet. TLS funciona en la capa de transporte del modelo TCP/IP, proporcionando una capa adicional de seguridad para los protocolos de la capa de aplicación que se ejecutan sobre él, como HTTP, SMTP y FTP. TLS utiliza criptografía de clave pública para proteger la información transmitida y autenticar a los servidores y usuario que están utilizando los dispositivos que se comunican. Además, este protocolo proporciona mecanismos para detectar y prevenir ataques de tipo DDOS " y otros tipos de amenazas a la seguridad.

- RSVP: Resource Reservation Protocol

Dado que la idea de la capa de transporte es llevar los paquetes a su destino, este protocolo nos permite que se almacene o reserver información de red específicos, como ancho de banda, para la transmisión de comunicaciones o servicios multimedia. Además, RSVP también permite que los routers y switches de la red reserven recursos para sesiones de comunicación de alta prioridad, asegurando así una experiencia de red más fluida y sin interrupciones.

- **Protocolos de la capa de aplicación:**
  - DNS: Domain Name Service

Este protocolo puede ser bien traducido al español como “Servicio para Nombres de Dominio”, este protocolo nos permite comunicarnos con nuestro lenguaje natural y humano con el internet, ¿a qué nos referimos? Cuando nosotros escribimos, por ejemplo https://www.google.com el protocolo DNS traduce este texto en una dirección IP correspondiente para poder ingresar al sitio dado que el internet funciona de esta manera, y el DNS nos facilita el acceso al poder ingresar con palabras y letras, en vez de las IP completas y correctas.

- FTP: File Transfer Protocol

FTP como bien su nombre lo indica, es un Protocolo de Transferencia de Archivos. Este protocolo funciona Servidor <-> Dispositivo, y funciona precisamente para esto, transferir archivos entre un servidor y un dispositivo y viceversa, además de ser utilizado como el protocolo idóneo para subida y descarga de archivos.

- TFTP: Trivial File Transfer Protocol

Este protocolo, igual que el protocolo FTP nos permite hacer tranferencia de archivos entre dispositivos, la principal diferencia con FTP son las capas de seguridad y validación, haciendo que TFTP sea muy util en redes locales y en la transferencia de archivos de confianza, además de ser utilizado para hacer la descarga, subida y transferencia de archivos de arranque entre dispositivos, y dado que se omiten las validaciones de seguridad es más eficiente y veloz. Podemos decir que es el UDP del FTP, quien sería el TCP.

- SNMP: Simple Network Management Protocol

Este protocolo, igual que los anteriormente mencionados, y los que siguen, tienen un nombre bastante explícito, y sin pensar más allá de las cosas, podemos definir concretamente este protocolo como el utilizado para monitorear cada uno de los dispositivos de la red, esto para tener un control sobre los recursos utilizados por cada uno de los dispositivos, poder encontrar fallas errores y obtener información para que la red y la comunicación entre dispositivos no falle.

- SMTP: Simple Mail Transfer Protocol

Este protocolo es el utilizado para la transmisión y/o transferencia de correos electrónicos entre dispositivos en una red. Este protocolo es útil ya que envía los correos directamente entre el dispositivo emisor y el receptor, y en algunos casos hay intermediarios, más sin embargo la idea del protocolo es poder tener la eficiencia para poder enviar correos entre dispositivos de una misma red.

- IMAP4: Internet Message Access Protocol version 4, revision 1

Este protocolo junto al protocolo SMTP permiten hacer gestión de correos electrónicos, en este caso el protocolo IMAP4 permite hacer uso de correos electrónicos en diferentes dispositivos de manera sincronizada, es decir, yo puedo redactar, recibir, leer, emitir, etc. Correos desde diferentes dispositivos y poder validarlo desde otro de manera sincronizada. Además este protocolo permite el uso de herramientas avanzadas de gestión de correos electrónicos.

- LDAP: Lightweight Directory Access Protocol

Este protocolo es el idóneo para poder gestionar y autenticar información de personas, en este caso, por ejemplo, nombre de usuarios, correos electrónico, etc. Y autenticar las identidades para que así se peuda tener un control sobre esta información y brindar una capa de seguridad sobre la información ya que muchos paquetes solo pueden ser entregados a personas específicas, en este caso identificadas y aseguradas por su LDAP. Debemos rescatar que LDAP es el protocolo que nos permite ingresar a los directorios que contiene esta información, y esta misma permitirá validar la autenticidad de los datos.

- NTP: Network Time Protocol

Este protocolo es util para poder brindar informació sobre el tiempo real en los sistemas y en las redes, util de manera empresarial para poder seguir un control sobre el manejo de la información y del flujo de trabajo en una institución y así poder validar correctamente en

función del tiempo cualquier actividad. Por ejemplo, en una red bancaria es util para poder consolidar la hora precisa de las transacciones. Este protocolo es util en el Internet ya que nos permite acceder de manera segura a varios sitios y es por esta misma razón que al querer ingresar al Internet con la hora desconfigurada de manera local, no podremos acceder correctamente.

- HTTP: HyperText Transfer Protocol

Dicho protocolo es la base de la transferencia de información en el internet, este protocolo es el que permite que los usuarios podamos entrar en contacto con prácticamente cualquier página web y solicitar información de las mismas. Tal como su nombre lo indica está relacionada con el HypetText Markup Language, ya que como bien lo indico este protocolo está directamente enlazado con las páginas web que en su totalidad tienen HTML en su creación. Hay que tener en cuenta que este protocolo funciona a través de los navegadores web, quienes solicitan la información de los servidores que nos proporcionarán la información de las páginas web, audios, videos, imagenes etc.

- HTTPS: HTTP over Secure Sockets Layer

Este protocolo a diferencia del HTTP, tiene una capa de seguridad e encriptamiento que permite que toda la información que nosotros como usuarios a través del navegador web brindamos, sea encriptada para que sólo el receptor tenga acceso a dicha información, así evitar que terceros puedan interceptar los datos y obtener beneficio de esto. Datos como contraseñas, tarjetas bancarias etc. Son encriptados siempre y cuando las páginas web tengan el protocolo HTTPS, en caso contrario los datos no serán encriptados siendo más vulnerables a la intercepción y obtención de estos datos. Hay que mencionar que la seguridad es brindada y proporcionada por otros dos protocolos, el TLS y SSL, el primero definido con anterioridad en los protocolos de la capa de transporte y el segundo será definido más adelante.

- DHCP: Dynamic Host Configuration Protocol

Este protocolo es el que permite que cualquier red pueda ser configurada con mayor facilidad haciendo uso de información de un servidor DHCP para poder validar direcciones IP y poder proporcionar a los dispositivos, direcciones IP automáticamente, además de otros datos como DNS; mascara, etc.

Dhcp, en resumidas cuenta es el protocolo que nos facilita la vida a la hora de configurar las direcciones IP de los dispositivos y estos datos técnicos para poder identificar dispositivos.

- SSL: Secure Sockets Layer

Este protocolo hace uso de criptografía para poder brindar seguridad a la información de la red y que sólo pueda ser leida por el receptor. Este protocolo permite que exista y funcione efectivamente el protocolo anteriormente definido, HTTPS. Hay que resaltar que este protocolo es usualmente utilizado en transacciones bancarias y asegurar la información, demostrando la efectividad de este portocolo y su fiabilidad.

Structured Cabling System (standards, services, applications)

"*Instalar una red de cables y un conjunto de conectores un número, una cantidad y una flexibilidad tales que permitan conectar dos puntos cualesquiera dentro de un edificio*" Cadenas Sanchez, X. & Zaballos Diego, A. (2015). *Guía de sistemas de cableado estructurado. P.22.*

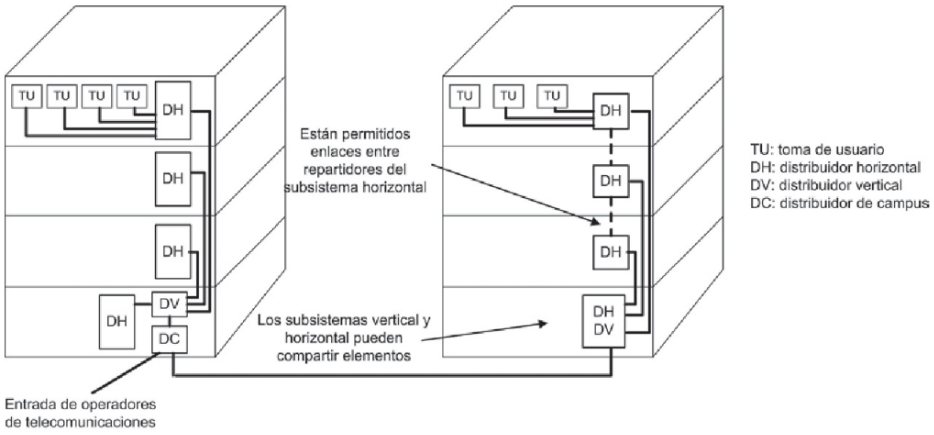

Figura 4. Estructura física de un sistema de cableado estructurado. tomada de Cadenas Sanchez, X. & Zaballos Diego, A. (2015). *Guía de sistemas de cableado estructurado. P.22.*

En una empresa u organización se suele tener una alta cantidad de equipos que se conectan a una red y esto genera una alta congestión y desorden por ello es necesario implementar una estructura adecuada para la instalación del cableado para formar la red de área local, para esto ya se han creado unos estándares que proveen orientación y facilitan significativamente la instalación y el mantenimiento de redes locales y a estos estándares se les llama "estándares de cableado estructurado".

Structures Cabling System o en español "Sistema de cableado estructurado" es un conjunto de elementos y equipos que, mediante el uso de productos de cableado y conectores, permite la integración de los servicios de voz, datos y video, junto con otros

sistemas de administración dentro de una edificación. De esta manera, se puede contar con una infraestructura unificada que cubra todas las necesidades de información y control en la edificación, incluyendo sistemas de seguridad, acceso y energía.

Las principales ventajas que tiene aplicar el sistema de cableado estructurado son:

- La independencia del cableado con la tecnología que se vaya a usar.
- Fácil administración de los cables,
- Menor costo del mantenimiento por lo fácil que es detectar los fallos.
- Con solo una instalación se tiene varias aplicaciones como los es voz, imagen y datos.
- Se puede tener en una sola toma todos los servicios de telecomunicación.
- Gracias a las normativas se tiene una calidad sin importar los fabricantes.
- Permite facil reubicación de los puestos.
- Mejor estética interna del edificio.

No todo es bueno y tambien tiene sus desventajas que son:

- Alta inversión inicial.
- Inversión a medio y largo plazo.
- Previamente se necesita un estudio para el diseño e instalación.

Como se dijo anteriormente esta estructura tiene unos estándares o normativas (recomendaciones o estándares industriales), que en caso de que no se cumplan estas normas hace que la instalación no soporte como es debido las aplicaciones esperadas. El estándar más usado fue desarrollado por “TIA” que significa “Telecommunication Industry Association” el estandar es TIA/EIA-568-A, tiempo después se publicó TIA/EIA-568-B, estos estándares son conocidos como “Norma de cableado de telecomunicaciones para edificios comerciales” y gracias a al éxito de este estandar se crearon otros si grandes cambios como lo es EN 50173, el estandar ISO/IEC 11801 y el UNE-EN 50173. A continuación, se mitrarán uno a uno indicando su lugar de uso.

- ISO/IEC 11801: Es la normativa publicada por ISO y con ámbito de aplicación mundial.
- ANSI/TIA/EIA: Es un estándar de la industria de EEUU.
- EN 50173: Ámbito español.
- IEEE 802.X: Normativas del ámbito industrial.

Las normativas empleadas por IEEE (Instituto de ingenieros Eléctricos y Electrónicos), se tiene en cuenta el cableado, topología física y eléctrica para redes locales, estos estándares fueron adoptados por la ISO (ISO 8802.X). Los estándares más conocidos son:

Estándar IEEE	Tecnología	Velocidad	Tipo de Cable
802.3	10BASE-5, 10BASE-2	10Mbps	Cable Coaxial
802.3i	10BASE-T	10Mbps	RJ-45 Cat 3
802.3u	100BASE-TX	100Mbps	RJ-45 Cat 5
802.3u	100BASE-FX	100Mbps	62.5µm MMF fibra
802.3z	1000BASE-CX	1000Mbps	2-pares, 150 ohm biaxial cable/DB-9
802.3z	1000BASE-LX	1000Mbps	62.5µm fibra multimodo 50µm fibra multimodo 9µ fibra monomodo
802.3z	1000BASE-SX	1000Mbps	62.5µm fibra multimodo 50µm fibra multimodo
802.3ab	1000BASE-T	1000Mbps	RJ-45 Cat 5e, 6
802.3ae	10GBASE-SR	10Gbps	62.5µm fibra multimodo 50µm fibra multimodo
802.3ae	10GBASE-LR	10Gbps	9µm fibra monomodo
802.3ae	10GBASE-ER	10Gbps	9µm fibra monomodo
802.3ae	10GBASE-LX4	10Gbps	9µm fibra monomodo 62.5µm fibra multimodo 50µm fibra multimodo
802.3ak	10GBASE-CX4	10Gbps	8 pares, 100 ohm biaxial cable
802.3an	10GBASE-T	10Gbps	Cat 6 aumentada (500MHz, U/UTP) (BORRADOR)

Figura 4.1. Estandares de IEEE 802.3. tomada de Cadenas Sanchez, X. & Zaballos Diego, A. (2015). *Guía de sistemas de cableado estructurado. P.38.*

Para el caso de Gigabit-Ethernet el esquema es diferente y la teclogia es la siguiente:

- 1000BaseLX: Emplea fibra óptica monomodo con alcance de 3Km y fibra optica multimodo con 550m.
- 1000BaseSX: Emplea fibra óptica multimodo con alcance de 275m o 550m.
- 1000BaseCX: Esta definida para cables de par trenzado de 150 ohm con distancia máxima de 25m.
- 1000BaseT: Esta definida para cables de par trenzado con distancia máxima de 100m.

En cuanto a los estándares EN, son regidas por la AENOR que es la Asociación Española de Normalización y Certificación, es miembro de las organizaciones internacionales ISO e IEC y CEN y CENELEC, lo que nos da a entender que las normas a seguir cuando se hace un proyecto de cableado estructurado son las hechas por ARNOR y la nomenclatura es UNE-EN-xxxxx y normativas mpas relevantes de esta son:

Norma EN 50173	Information technology - Generic cabling systems
prEN 50173-1:2005	Part 1: General requirements
prEN 50173-2:2005	Part 2: Office premises
prEN 50173-3	Part 3: Industrial premises
prEN 50173-4:2005	Part 4: Residential premises
prEN 50173-5:2005	Part 5: Data centers

Norma 50174	Information technology - Cabling installation
EN 50174-1:2000	Part 1: Specification and quality assurance
prEN 50174-1	Part 1: Specification and quality assurance
EN 50174-2:2000	Part 2: Installation planning and practices inside buildings
prEN 50174-2	Part 2: Installation planning and practices inside buildings
EN 50174-3:2003	Part 3: Installation planning and practices outside buildings

Figura 4.2. Estándares de EN. tomada de Cadenas Sanchez, X. & Zaballos Diego, A. (2015). *Guía de sistemas de cableado estructurado. P.45.*

Las fases de los proyectos de cableado tienen una normativa que las guía como se puede observar y cada esta impone un estándar de calidad. Los sistemas de cableado estructurado aparte de sus estándares tienen unos elementos que permiten que ofrezca los servicios supuestos estos elementos son:

- Repartidor: Se usa para distribuir el cableado y solo puede haber uno.
- Backbone de campus: Este une los edificios que hacen parte de la infraestructura.
- Distribuidor vertical: Distribuye el cableado de manera vertical en el edificio.
- Cableado vertical: Interconecta los subsistemas horizontales.
- Distribuidor horizontal: Es donde está el cableado horizontal.
- Cableado horizontal: Este conecta los puestos de trabajo de todo el sistema cableado.
- Toma de usuario: En el punto en el que el usario se conecta a la red cableada.
- Sala de equipos: Es donde están los equipos de interconexión, como los servidores, los routers, switches, entre otros.

La estructura logica del sistema de cableado estructurado tiene una forma de jerárquia como la siguiente:

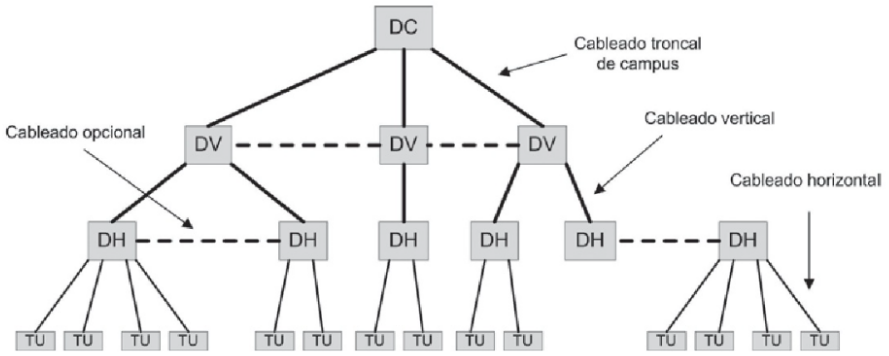

Figura 4.3. Estructura lógica de un sistema de cableado estructurado. tomada de Santos González, M. & Moreno Pérez, J. C. (2015). *Sistemas informáticos y redes locales. P.210.*

Para entender mejor esto de los subsistemas está el subsistema de distribución de campus en el cual se da unión a los edificios y los medios usados son fibra óptica y radio enlaces, en el subsistema de distribución horizontal se tienen elementos como el cableado horizontal que son los cables que van en canaletas, techo o por un suelo falso, para estos se tienen los "latiguillos" que son cables UTP de conexión RJ-45, estos hacen de cable de union y se ven asi:

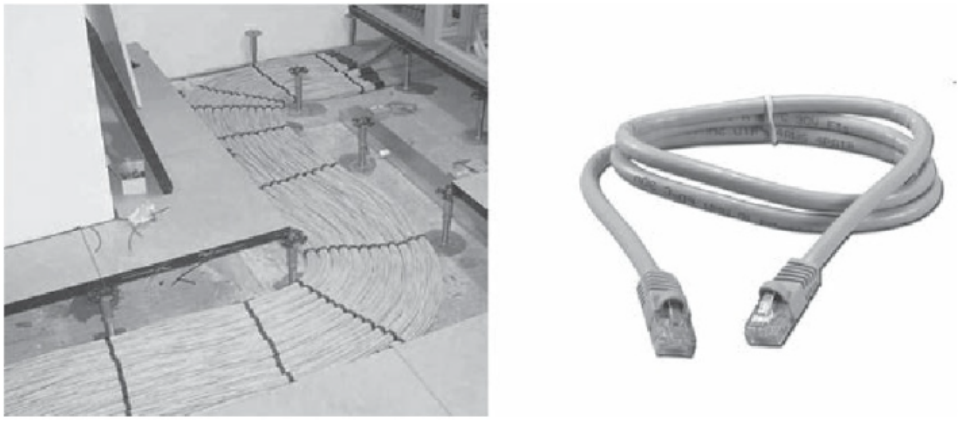

Figura 4.4. Cableado horizontal y un latiguillo de red. tomada de Santos González, M. & Moreno Pérez, J. C. (2015). *Sistemas informáticos y redes locales. P.210.*

Para poder emplear estos se hace uso de las rosetas que son las conexiones hembra de los conectores RJ-45. Para la instalación y certificación del sistema de cableado estructurado se hace necesario el uso de un armario de comunicaciones que es donde está el distribuidor horizontal y la electrónica de red.

Los servicios que brinda como ya se vio son la transmisión de voz permitiendo señales de alta calidad gracias a los cables y conectores que establecen conexiones confiables, transmisión de datos por la capacidad de transmitir a altas velocidades y con grandes cantidades de información, transmisión de video por lo ya mencionado anteriormente es más que evidente que también transmitir video de alta calidad para funciones como videoconferencias, monitoreo de seguridad y señalización digital,

seguridad y control de acceso es otro servicio que puede brindar ya que permite la implementación de cámaras de vigilancia, alarmas y lectores de tarjeta de identificación, que se integran en la red de comunicaciones y por último servicio está el sistemas de energía ya que por sus sistemas de distribución se pueden incluir sistemas de alimentación de energía eléctrica para los equipos de comunicación, garantizando un funcionamiento ininterrumpido.

Por tanto, a las aplicaciones que tiene son varias como edificios, centros comerciales, hospitales, fábricas, escuelas, universidades y entre otros ya que el sistema de cableado estructurado está presente en redes de computadoras, en la comunicación de voz, en videoconferencias, sistemas de seguridad, automatización de edificios y señalización digital como lo son pantallas informáticas y publicidad.

La topología manejada en estas redes es:

- **Topología de bus**

Es un sistema típico de las redes antiguas, en la que un cable coaxial hacía de vertebra y todos los dispositivos estaban conectados a este siendo el único medio compartido.

- **Topología de anillo**

Es empleada en cualquier red WAN con fibra óptica, en esta todos los dispositivos están conectados entres si formando una especio de bucle.

- **Topología en estrella.**

Es la topología más usa en las redes LAN, llego remplazando a la topología bus y la anillo por la eficiencia que esta mostraba, en esta se forma un nodo en el centro del cual salen todos los enlaces hacia las periferias.

- **Topología en estrella extendida.**

Es la evolución de la topología en estrella, siendo una estrella central en la cual los nodos exteriores tienen otros nodos que conectan a varios equipos en simultaneo.

- **Topología en malla.**

En esta todos los dispositivos se conectan entre sí por conexión punto a punto.

- **Topología en árbol.**

Este es una topología utilizada normalmente en redes empresariales ya que la gestión que permite es centralizada, es escalable y modular, por lo que para redes complejas es idónea. Esta topología plantea una red en la que los nodos están estructurados de tal manera que simula un árbol jerárquico. Hay un nodo raíz en la parte superior y cada uno de los demás se ramifican desde este, y cada nodo tiene hijos, pero solo un padre.

- **Topología híbrida.**

Este tipo de topología es una en la que se conectan entre sí diferentes tipos de topologías como la topología de estrella, de malla, en árbol etc. Así formando una red más grande. Estas diferentes topologías pueden ser conectadas a través de switches, enrutadores o puentes y pueden ser cableada o inalámbricas.

Conclusión

Como vimos a través del análisis, investigación e implementación de lo aprendido a través de Cisco Packet Tracer, y realizando la debida lectura de la información necesaria, hemos podido concluir que a través de la evolución tecnológica y del internet, las redes no son ajenas a todo lo que está detrás, refiriéndonos a los protocolos y estándares, teniendo presente que no sólo nos competen las redes y su parte física en sí sino todo lo que está alrededor de esto. De nada nos sirve un cableado estructurado correctamente sin un protocolo con el cuál poder transmitir la información de manera efectiva y correcta, y de misma manera de nada nos sirve tener protocolos y teoría sin un medio físico que haga uso de esto. Además, debemos destacar que cada uno de los elementos que se implementan en las redes pueden ser de diferentes tipos y que cumplen diferentes funciones, debemos tener en cuenta la cantidad de herramientas y servicios diferentes con los que contamos y que podemos emplear en cada uno de nuestros futuros proyectos. Teniendo buenas bases teóricas tendremos las habilidades para poder definir qué métodos, estándares, protocolos usar y qué parte física o elementos de transmisión funcionarán con dichos estándares. Cada uno de los elementos estudiados e investigados en este trabajo nos ha permitido ampliar nuestros conocimientos y volvernos más competentes en nuestra área, y nos ha brindado lo necesario para tener cada vez una visión más amplia de nuestra labor, y de que no sólo existe una manera de crear una red, y no existe una sola manera de implementar la transmisión de la información, de la seguridad y de la eficiencia de cada tipo de red, además de las técnicas y métodos que ya han sido desarrollados y que nosotros tenemos la facilidad de acceso al conocimiento para implementarlos.

Referencias bibliográficas

- Kurose, J. F. & Ross, K. W. (2010). Redes de Computadoras: Un enfoque descendente basado en Internet (5ª ed.). Pearson.

- Kurose, J. F. & Ross, K. W. (2013). Redes de Computadoras: Un enfoque descendente basado en Internet (6ª ed.). Pearson.

- Sánchez Rubio, M. Barchino Plata, R. & Martínez Herráiz, J. J. (2020). Redes de computadores. Editorial Universidad de Alcalá. https://elibro-net.bdbiblioteca.universidadean.edu.co/es/lc/bibliotecaean/titulos/131606

- Caffa, A. (2016). Conceptos de redes de computadoras. D - Universidad de la República. https://elibro-net.bdbiblioteca.universidadean.edu.co/es/lc/bibliotecaean/titulos/31007

- Stallings, W. (2014). Comunicaciones y redes de computadores (9ª ed.). Pearson.

- Tanenbaum, A. S., & Wetherall, D. J. (2012). Redes de computadoras. Pearson Educación.

- Forouzan, B. A. (2012). Comunicación de datos y redes de computadoras (Cuarta ed.). McGraw-Hill

- Forouzan, B. A. (2013). Data Communications and Networking. McGraw-Hill Education.

- Leiden, C., & Wilensky, M. (2009). *TCP / IP For Dummies* (6th ed.). John Wiley & Sons.

- Barnett, D. & McBee, J. (2014). Cabling: The Complete Guide to Network Wiring. Sybex

- Cadenas Sanchez, X. & Zaballos Diego, A. (2015). *Guía de sistemas de cableado estructurado.*. Ediciones Experiencia. https://elibro-net.bdbiblioteca.universidadean.edu.co/es/lc/bibliotecaean/titulos/41979

- Santos González, M. & Moreno Pérez, J. C. (2015). *Sistemas informáticos y redes locales.*. RA-MA Editorial. https://elibro-net.bdbiblioteca.universidadean.edu.co/es/lc/bibliotecaean/titulos/62492