La Enumeración de los componentes y su uso:

El Servidor:

Generalmente se trata de una computadora o aplicación encargada de proveer a otros equipos de unos determinados servicios, como el almacenamiento de información. Se encarga de procesar las solicitudes de esos otros equipos, que en ocasiones se denominan clientes, a los que les entregan datos por medio de una red que puede ser local o por Internet.

La estación de trabajo:

Es el equipo informático destinado a realizar una determinada labor profesional, técnica o científica. En resumen, en una oficina, las estaciones serían cada uno de los ordenadores con los que se lleva a cabo el trabajo y que generalmente están conectadas entre sí a través de un servidor para facilitar los flujos de información, conectadas a periféricos (como impresoras, escáneres, pantallas de proyección, etc.) y a la vez conectadas a Internet.

La tarjeta de conexión a la red:

por lo general está integrada dentro del equipo o estación de trabajo, permitiendo que éste pueda conectarse a una determinada red, mediante programas controladores compatibles con los protocolos y características del sistema operativo.

El repetidor:

permiten retransmitir una señal de red débil o de bajo nivel de forma amplificada a una potencia superior. El funcionamiento y características de los repetidores dependerán también del tipo de red que se esté utilizando, por ejemplo si es por cable o por wifi.

Los bridgets o puentes de red:

son dispositivos de interconexión de segmentos de redes. Básicamente se encargan de crear una sola subred conectando equipos sin necesidad de router, a través de segmentos de red que a su vez ya están conectando a diversos equipos.

Los hubs:

permiten conectar múltiples dispositivos mediante cables, consiguiendo que funcionen como un único segmento de red. La traducción al castellano de este término es “cubo” o “concentrador” y así es como realmente funcionan, concentrando en un mismo aparato la conexión múltiple de, por ejemplo, televisores, USB, tarjetas SD, ordenadores, etc.

Actúan como centralizadores de conexión en una red, conectando eléctricamente todos los puertos de entrada, compartiendo información simultáneamente para que todos los dispositivos conectados puedan acceder a ella.

El switch:

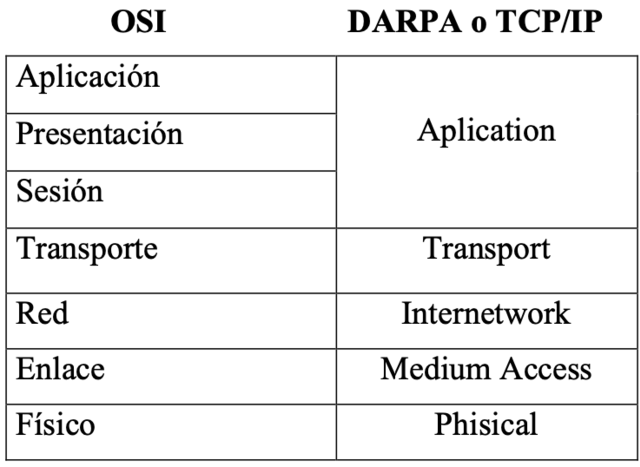
son dispositivos digitales que se encargan de interconectar dos o más segmentos de red, de forma similar a como lo hacen los bridgets, otros componentes de redes que te explicamos anteriormente. Permiten formar lo que se conoce como una red de área local (LAN, Local Area Network), cuyas especificaciones técnicas siguen el estándar denominado Ethernet.

El router:

El “enrutador”, ya que se encarga de alguna manera de encontrar el mejor camino para la transmisión de información a través de una red. Sus usos pueden ser más o menos complejos aunque el más común es aquel que permite a varios equipos, ya sea en casa o en una oficina, aprovechar la misma conexión a Intenet

recibiendo la conexión de red y distribuyéndola a todos los dispositivos conectados simultáneamente escogiendo la mejor vía para hacerlo de forma que la información completa llegue de manera adecuada y en el menor tiempo posible.

La enumeración de los protocolos TCPIP:



Nivel de Aplicación (Application Layer):

Protocolos TCP/IP: HTTP, HTTPS, FTP, SMTP, DNS, etc.

Modelo OSI: Capa de Aplicación.

Nivel de Transporte (Transport Layer):

Protocolos TCP/IP: TCP (Transmission Control Protocol), UDP (User Datagram Protocol).

Modelo OSI: Capa de Transporte.

Nivel de Red (Internet Layer):

Protocolos TCP/IP: IP (Internet Protocol), ICMP (Internet Control Message Protocol).

Modelo OSI: Capa de Red.

Nivel de Acceso a la Red (Link Layer):

Protocols TCP/IP: Ethernet, PPP (Point-to-Point Protocol), ARP (Address Resolution Protocol).

Modelo OSI: Capa de Enlace de Datos.

A continuación, proporcionaré una explicación más detallada:

1. Nivel de Aplicación:

Este nivel se encarga de proporcionar servicios de red directamente a las aplicaciones del usuario. Incluye protocolos que permiten la comunicación entre aplicaciones.

2. Nivel de Transporte:

Es responsable de la entrega de datos de extremo a extremo y proporciona la detección y corrección de errores, así como el control de flujo. TCP garantiza la entrega ordenada y sin errores, mientras que UDP es más ligero y no garantiza la entrega ni el orden.

3. Nivel de Red:

Este nivel se ocupa del enrutamiento de los datos a través de la red. El protocolo IP es crucial en esta capa para asignar direcciones y enrutar los paquetes correctamente.

4. Nivel de Acceso a la Red:

Se encarga de la transferencia confiable de datos entre nodos de red adyacentes y proporciona la interfaz entre la capa de red y el medio físico. Incluye protocolos y tecnologías específicas de acceso a la red, como Ethernet o Wifi.

Modelo de Referencia OSI:

El modelo de referencia OSI (Open Systems Interconnection) es un marco conceptual que divide las funciones de una red de computadoras en siete capas. Cada capa realiza funciones específicas y se comunica con las capas adyacentes para facilitar la transmisión de datos a través de una red. Aunque el modelo OSI es teórico, proporciona una base estructurada para comprender cómo interactúan los componentes de una red.

La segmentación y encapsulación:

Segmentación:

La segmentación es un proceso en el que los datos de una capa superior se dividen en segmentos más pequeños antes de ser transmitidos a través de una red. Este proceso es particularmente relevante en el contexto de la capa de transporte, donde los datos pueden ser de tamaño considerable y necesitan ser divididos en segmentos para su transmisión eficiente.

Proceso Técnico de Segmentación:

Capa de Aplicación/Transporte: En el nivel de la capa de transporte, los datos generados por las aplicaciones se dividen en segmentos más pequeños. Por ejemplo, si estás enviando un archivo grande, este se divide en segmentos más manejables.

División en Segmentos: La capa de transporte, especialmente en el caso de TCP, divide los datos en segmentos de un tamaño específico. Cada segmento lleva información sobre su posición relativa en la secuencia total y otros datos de control.

Numeración de Secuencia: Cada segmento se numerará secuencialmente para que, en el extremo receptor, se pueda reorganizar correctamente la secuencia original de los datos.

Envío a Capa de Red: Los segmentos se pasan luego a la capa de red para su posterior transmisión a través de la red.

Encapsulación:

La encapsulación es el proceso de agregar encabezados (headers) y, en algunos casos, trailers a los datos en cada capa a medida que atraviesan la pila de protocolos. Cada capa agrega su propia información de control a los datos, creando así una "cáscara" alrededor de los datos originales. Esta cáscara se quita en cada capa correspondiente en el extremo receptor.

Proceso Técnico de Encapsulación:

Capa de Aplicación: Los datos de la aplicación se encapsulan con un encabezado que contiene información sobre el tipo de aplicación y otros datos relevantes.

Capa de Transporte: Cada segmento, generado durante la segmentación, se encapsula con un encabezado que contiene información sobre el control de flujo, la detección de errores y la numeración de secuencia (en el caso de TCP).

Capa de Red: En la capa de red, se agrega un encabezado que incluye información de direccionamiento IP, permitiendo la correcta entrega de los datos a través de la red.

Capa de Enlace de Datos: Finalmente, en la capa de enlace de datos, se agrega un encabezado y, posiblemente, un tráiler, que contiene direcciones de hardware (MAC) y otros datos necesarios para la transmisión física de datos.

Desencapsulación en el Receptor:

En el extremo receptor, los encabezados y trailers se van eliminando sucesivamente a medida que los datos atraviesan las capas de la pila de protocolos, hasta que los datos originales de la aplicación son recuperados.

Los medios de Transmisión de los hosts:

Cable de Par Trenzado:

Descripción: Es uno de los medios más utilizados para la transmisión de datos. Consiste en pares de cables de cobre trenzados entre sí. Hay dos tipos principales: par trenzado no apantallado (UTP) y par trenzado apantallado (STP). El UTP se utiliza comúnmente en redes Ethernet.

Cable Coaxial:

Descripción: Este tipo de cable tiene un conductor central rodeado por una capa aislante, una malla metálica y una cubierta externa. Se utiliza en aplicaciones como la transmisión de señales de televisión por cable y en algunas redes de área local (LAN).

Fibra Óptica:

Descripción: Utiliza pulsos de luz para transmitir datos. La fibra óptica consiste en hebras delgadas de vidrio o plástico que transmiten luz a lo largo de distancias considerablemente largas. Es conocida por su alta velocidad y capacidad para transmitir grandes cantidades de datos.

Ondas de Radio (Inalámbrico):

Descripción: La transmisión inalámbrica utiliza ondas de radio para la comunicación entre dispositivos. Esto incluye tecnologías como Wi-Fi, Bluetooth y las comunicaciones móviles. Es especialmente útil en situaciones donde el tendido de cables no es práctico.

Satélites:

Descripción: La comunicación vía satélite utiliza satélites en órbita para retransmitir señales entre dos puntos en la Tierra. Es común en aplicaciones como las transmisiones de televisión por satélite y las comunicaciones globales.

Líneas Eléctricas:

Descripción: En algunos casos, las líneas eléctricas se han utilizado para la transmisión de datos mediante tecnologías como Power Line Communication (PLC). Esto implica la superposición de señales de datos en las líneas eléctricas existentes.

Medios Guiados vs. No Guiados:

Medios Guiados: Incluyen aquellos en los que las señales viajan a lo largo de un camino físico, como cables de cobre o fibra óptica.

Medios No Guiados: Incluyen aquellos en los que las señales se propagan a través del aire o del espacio libre, como las ondas de radio.

Selección del Medio de Transmisión:

La elección del medio de transmisión depende de varios factores, como la distancia que debe cubrir la transmisión, la velocidad requerida, la interferencia ambiental, el costo y otros requisitos específicos del entorno de red.

El funcionamiento de la capa de red e IP:

Enrutamiento:

La capa de red decide la ruta que los datos seguirán desde el origen hasta el destino a través de una serie de dispositivos llamados routers. Cada dispositivo en una red tiene una dirección única conocida como dirección IP, y los routers utilizan esta información para determinar la mejor ruta para los datos.

Direccionamiento:

La dirección IP es esencial en la capa de red. Cada dispositivo conectado a la red tiene una dirección IP única que se utiliza para identificarlo en la red. La dirección IP se divide en dos partes: la parte de red y la parte de host, lo que permite la segmentación y organización de dispositivos en redes más grandes.

Fragmentación y Reensamblaje:

La capa de red maneja la fragmentación y el reensamblaje de datos cuando es necesario dividir paquetes en segmentos más pequeños para ser transmitidos eficientemente a través de la red. Esto es especialmente importante cuando los datos son demasiado grandes para ajustarse en el tamaño máximo permitido por la red o cuando los diferentes segmentos de datos toman rutas diferentes.

Control de Congestión:

La capa de red también está involucrada en el control de la congestión en la red. Utiliza técnicas como el ajuste del flujo de datos y la señalización para garantizar un flujo eficiente y evitar la saturación de la red.

Funcionamiento de la Capa de Red e IP:

Encapsulación:

Cuando los datos viajan a través de la pila de protocolos, en la capa de red, se encapsulan en un paquete de red. Este paquete incluye información como la dirección IP de origen y destino, y otros campos necesarios para el enrutamiento y la entrega adecuada.

Enrutamiento:

Los routers en la red examinan la dirección IP de destino en el paquete y toman decisiones sobre cómo dirigir el paquete hacia su destino. Utilizan tablas de enrutamiento para determinar la mejor ruta.

Fragmentación (si es necesario):

Si el tamaño del paquete excede el límite permitido en la red, la capa de red puede fragmentar el paquete en segmentos más pequeños. Esto asegura que los datos se transmitan eficientemente a través de la red y se reensamblarán en el destino.

Desencapsulación en el Destino:

En el destino, la capa de red en el dispositivo receptor desencapsula el paquete, exponiendo los datos originales a la capa superior de transporte.

Entrega a Capas Superiores:

Finalmente, los datos se entregan a las capas superiores de la pila de protocolos para su procesamiento adicional.

La conformación de las direcciones de IPv4 clase A,B,C:

Clase A:

Rango de Direcciones: 1.0.0.0 a 126.255.255.255

Formato de Dirección: NNN.HHH.HHH.HHH

En la clase A, el primer octeto (NNN) representa la parte de red, mientras que los tres octetos restantes (HHH) representan la parte de host. Esto permite un gran número de redes con un gran número de hosts por red. El rango de direcciones es extenso, pero debido a la estructura, hay un número limitado de redes posibles.

Clase B:

Rango de Direcciones: 128.0.0.0 a 191.255.255.255

Formato de Dirección: NNNN.NNNN.HHH.HHH

En la clase B, los dos primeros octetos (NNNN) representan la parte de red, mientras que los dos octetos restantes (HHHH) representan la parte de host. Esto permite un número moderado de redes con un número moderado de hosts por red. La clase B es comúnmente utilizada por organizaciones más grandes.

Clase C:

Rango de Direcciones: 192.0.0.0 a 223.255.255.255

Formato de Dirección: NNNN.NNNN.NNN.HHH

En la clase C, los tres primeros octetos (NNNN.NNNN.NNN) representan la parte de red, mientras que el último octeto (HHH) representa la parte de host. Esto permite un gran número de redes, pero con un número más limitado de hosts por red. La clase C es comúnmente utilizada por redes más pequeñas.

La máscara de subred y su funcionamiento:

La máscara de subred consiste en una serie de bits "1" seguidos de una serie de bits "0". La parte de "1" indica la porción de red de la dirección IP, y la parte de "0" indica la porción de host. Los bits "1" y "0" se representan comúnmente en formato decimal con cuatro octetos, similar a una dirección IP.

Ejemplo:

Máscara de subred para una red de clase C: 255.255.255.0

Representación binaria: 11111111.11111111.11111111.00000000

En este ejemplo, los primeros 24 bits (los primeros tres octetos) se utilizan para identificar la red, y los últimos 8 bits (el último octeto) se utilizan para identificar hosts dentro de esa red.

Funcionamiento de la Máscara de Subred:

División de Redes:

La máscara de subred divide una dirección IP en dos partes: la parte de red y la parte de host. La longitud de la máscara (el número de bits "1") determina cuántos bits se utilizan para la parte de red y, por lo tanto, cuántos bits quedan para la parte de host.

Identificación de la Red y Host:

Al aplicar la máscara de subred a una dirección IP, se obtiene la dirección de red. Esto se hace realizando una operación lógica AND bit a bit entre la dirección IP y la máscara de subred. El resultado es la dirección de red. La parte de host de la dirección IP se mantiene sin cambios.

Ejemplo:

Dirección IP: 192.168.1.25

Máscara de Subred: 255.255.255.0

Operación AND: 192.168.1.25 AND 255.255.255.0 = 192.168.1.0 (Dirección de red)

Identificación de Hosts en la Red:

Los hosts dentro de la misma red tendrán la misma dirección de red. La variación en la parte de host permitirá identificar dispositivos individuales en esa red. Dado que la longitud de la máscara determina cuántos bits están disponibles para la parte de host, también determina el número máximo de hosts posibles en esa red.

Ejemplo:

Si la máscara es /24 (255.255.255.0), hay 256 direcciones posibles en la red (2^8), pero se restan dos (la dirección de red y la de broadcast), por lo que hay 254 direcciones disponibles para hosts.