

Contenido

<u>1.1. DEFINIR RED DE COMPUTADORAS.</u>	2
<u>1.2. VENTAJAS DE CONECTAR COMPUTADORAS.</u>	3
<u>1.3. DEFINIR ARQUITECTURA DE RED.</u>	4
<u>1.4. DEFINA Y DESCRIBA MODELO OSI.</u>	8
<u>1.5. DEFINA TIPOS DE REDES SEGÚN:</u>	10
<u>1.6. EXTENSIÓN</u>	10
<u>1.6.1. LAN</u>	10
<u>1.6.2. MAN</u>	10
<u>1.6.3. WAN</u>	11
<u>1.7. FUNCIÓN.</u>	12
<u>1.7.1. SERVIDOR. PEER TO PEER?</u>	12
<u>1.7.2. CLIENTE – SERVIDOR.</u>	12
<u>1.8. CONEXIÓN FÍSICA.</u>	12
<u>1.8.1. INALÁMBRICA.</u>	13
<u>1.8.2. INALÁMBRICA (BLUETOOTH-WIFI)</u>	26
<u>1.8.2.1. TOPOLOGÍA</u>	27
<u>1.8.2.2. BUS, TRONCAL</u>	28
<u>1.8.2.3. ESTRELLA</u>	30
<u>1.8.2.4. ESTRELLA, TRONCAL</u>	31
<u>1.9. COMUNICACIÓN(PROTOCOLOS)</u>	31
<u>1.9.1. TCP/IP (TRANSFER CONTROL PROTOCOL/INTERNET PROTOCOL)</u>	42
<u>1.9.2. DEFINA QUE ES UNA IP</u>	44
<u>1.9.3. DIFERENCIA IP ESTATICA Y DINAMICA</u>	49
<u>1.9.4. DIFERENCIA IP RESERVADA (PRIVADA, PUBLICA)</u>	50
<u>1.9.5. DIFERENCIA IPV4, IPV6</u>	51
<u>1.9.6. DEFINA CLASES DE DIRECCIONES IP (A, B, C, D, E)</u>	54
<u>1.9.7. CONCEPTO DNS (DOMAIN NAME SYSTEM)</u>	58
<u>1.9.8. CONCEPTO PUERTA DE ENLACE</u>	58
<u>1.9.9. CONCEPTO DHCP</u>	60
<u>1.9.10. CONCEPTO MASCARA DE SUBRED</u>	60
<u>1.9.11. COMANDOS IP</u>	61

Nro. Grupo:2

<u>1.9.11.1. DESCRIBA IPCONFIG</u>	62
<u>1.9.11.2. DESCRIBA PING</u>	62
<u>2. MAQUINA VIRTUALES</u>	64
<u>2.1. DEFINICIÓN DE MÁQUINA VIRTUAL (VIRTUAL MACHINE)</u>	64
<u>2.2. PARA QUE SIRVE UNA MAQUINA VIRTUAL</u>	65
<u>2.3. TIPOS DE MÁQUINAS VIRTUALES</u>	65
<u>2.3.1. MÁQUINAS VIRTUALES DE SISTEMA</u>	65
<u>2.3.2. MÁQUINAS VIRTUALES DE PROCESO</u>	66
<u>2.4. DIFERENCIA ENTRE DISCO ESTÁTICO Y DINÁMICO</u>	67

1.1. DEFINIR RED DE COMPUTADORAS.

Una red de computadoras es un conjunto de computadoras interconectadas entre sí a través de un medio, las cuales intercambian información y comparten recursos. En una comunicación podemos encontrar dos roles definidos como Emisor y Receptor, estos intercambian mensajes entre sí.

- **Dispositivos:** Los dispositivos que se conectan a una red informática, pueden clasificarse en: los gestores de acceso (módem, router, switch, etc) y realizan las comunicaciones y los que se conectan entre sí (computadora, notebook, impresora, etc).

Arquitectura Cliente/Servidor:

Servidor: el dispositivo brinda un servicio.

Cliente: el dispositivo consume el o los servicios de el o los dispositivos servidores.

Arquitectura *peer to peer*:

También llamada punto a punto, los dispositivos pueden tomar ambos roles, tanto cliente como servidor en simultáneo.

- **Medio de comunicación:** a través de este se hace posible la comunicación entre dispositivos.

Guiado o dirigido: con las ondas que se transmiten y son guiadas a través de un

canal físico o cable, estos son el cable coaxial, cable par trenzado y fibra óptica.

No guiados: estas ondas son inalámbricas, estos medios son Wifi y Bluetooth (ondas de radio), las ondas infrarrojas y las microondas.

- **Información:** son los datos que se transmiten entre los dispositivos (texto, imágenes, música, video, etc.)

- **Recursos:** todo lo que un dispositivo solicita a la red, pudiendo ser identificado y accedido directamente, como archivos compartidos desde otro dispositivo, otro servicio, una impresora, un documento, espacio en un HDD, etc.

1.2. VENTAJAS DE CONECTAR COMPUTADORAS.

Nro. Grupo:2

- **Comunicación más rápida, eficiente y ahorro de costos.**

El uso de redes agiliza la comunicación entre dispositivos que se pueden encontrar lejanos. Por ejemplo, el acceso a una computadora que tiene información a la que acceden otras. El correo electrónico y la mensajería instantánea son herramientas que nos proveen de comunicación entre usuarios que se encuentran lejanos, en forma rápida y efectiva.

- **Posibilidad de compartir software, hardware e intercambio de información.**

Se pueden compartir dispositivos costosos para que un mismo dispositivo sea utilizado por otros. Un ejemplo podría ser el uso de una impresora por varias computadoras de forma simultánea.

- **Control del dispositivo de forma remota.**

Podemos acceder a un dispositivo desde otro y manejarlo de forma remota.

- **Comunicaciones personales**

Podemos comunicarnos con personas de todo el mundo a través de las redes con el uso de internet.

- **Mejora la seguridad y control de la información que se utiliza e intercambia.**

El acceso a la información puede ser administrado para cada uno de los dispositivos utilizando configuraciones de acceso para cada uno de ellos y así gestionar la información que será visible.

- **Informatización de trámites y confiabilidad en la información oficial.**

Muchos de los trámites que antes eran presenciales ahora se vieron alcanzados por la era digital y a través de internet se pueden realizar gestiones en organismos oficiales por esta vía. Además, el acceso a plataformas oficiales y así a la información actualizada y confiable.

1.3. DEFINIR ARQUITECTURA DE RED.

Nro. Grupo:2

La arquitectura de red se refiere a las tecnologías que admiten la infraestructura y a los servicios y protocolos para la transmisión de la información en una red. Podemos definirla por las siguientes características:

- **Topología:** se trata de la ubicación física de equipos de telecomunicaciones y cableado de conexión entre dispositivos. Define la interconexión de las estaciones y la transmisión de datos en el medio de comunicación.

Topología física: ubica a los dispositivos (hosts) dentro de la red, entre ellos se encuentran: tipología bus, anillo, doble anillo, estrella, estrella extendida, árbol o jerárquica, malla y mixta.

Topología lógica: se refiere a las conexiones virtuales entre los dispositivos. Existen dos tipos de accesos al medio: difusión o **Broadcast** y pase testigo o **Token**.

- **Protocolo de comunicaciones:** conjunto de reglas para la comunicación entre

dispositivos de una red. Reglas de identificación entre dispositivos y de formateo para saber si la información es enviada y recibida de forma correcta.

Protocolos de Capa de enlace de Datos (Capa 2- Acceso a los medios): Recibe peticiones de la capa 3 y utiliza los servicios de la capa 1 (capa física).

- **Address Resolution Protocol (ARP):** es un protocolo de internet y de redes locales. También trabaja con el protocolo IP para mapear direcciones IP en relación a las direcciones de hardware o MAC (código de identificación de interfaces de red de dispositivos). Opera entre la capa de red y la de acceso al medio. Se aplica cuando utilizamos protocolo IP sobre Ethernet.

- **Protocolo punto a punto (PPP):** conecta dos enrutadores directamente sin ningún equipo u otro dispositivo de red entre medias de ambos.

Nro. Grupo:2

- **Protocolo de enlace de alto nivel (HDLC):** Recuperación de errores en caso pérdida de paquetes de datos, fallos de secuencia y otros, ofrece una comunicación confiable entre el transmisor y el receptor.

Protocolos de Capa de Red (Capa 3 – Direccionamiento y mejor ruta): proporciona conectividad y selección de ruta entre dos sistemas hosts. Tipos de servicios:

Servicios no orientados a la conexión (CLNS): Cada paquete debe llevar la dirección de destino, los nodos de la red deciden qué camino deben seguir.

Servicios orientados a la conexión (CONS): solo el primer paquete de cada mensaje lleva la dirección de destino.

- **Internet Protocol (IP):** protocolos de internet que determinan la manera en que se transmiten los datos a través de la red. Especificaciones de cómo deben funcionar los dispositivos conectados:

§ **Direccionamiento:** asegura que cualquier dispositivo conectado cuente con una dirección IP y así se asegure el conocimiento del origen y destino de la información

siempre que se requiera.

§ **Routing:** determinar el camino de la información basándonos en la dirección IP.

- **Internet Control Message Protocol (ICMP):** control de errores, reporte y consultas de gestión. Es un protocolo utilizado por dispositivos como routers para enviar mensajes de errores e información relacionada con las operaciones.
- **OSPF** (Open Shortest Path First): encaminamiento jerárquico, calcula la ruta más corta entre dos nodos.
- **IS-IS** (Intermediate System to Intermediate System).
- **IGMP** (Internet Group Management Protocol).

Protocolos de Capa de Transporte (Capa 4 – Conexión de extremo a extremo): encargado de la transferencia libre de errores de los datos entre emisor y receptor. Servicios a capas superiores: Orientado y no orientado a la conexión.

Orientado a la conexión: establecimiento, transferencia de datos y liberación.

No orientado a la conexión: se tratan los paquetes de forma individual.

La interfaz del servicio de la capa de transporte proporciona las siguientes operaciones a los programas de aplicación: **LISTEN:** Se bloquea hasta que algún proceso intenta el contacto. **CONNECT:** Intenta activamente establecer una conexión. **SEND:** Envía información. **RECEIVE:** Se bloquea hasta que llegue una TPDU de DATOS. **DISCONNECT:** Este lado quiere liberar la conexión.

- **Transmission Control Protocol (TCP):** conjuntamente con el IP, se asegura que la información se transmita de forma adecuada a través de internet, que ésta llegue a destino de forma confiable. Otras de sus funciones son: evitar que se pierda información a la hora de ser enviada, controlar el orden de la información y prevención de información duplicada.

- **User Datagram Protocol (UDP):** este protocolo es menos utilizado que el TCP ya que no cuenta con la posibilidad de realizar revisiones en búsqueda de errores y correcciones de transmisiones de información. Este protocolo es utilizado en escenarios de juegos en línea o sesiones de streaming ya que es más rápido.

Protocolos de Capa de Sesión (Capa 5 – Comunicación entre hosts): proporciona los mecanismos para controlar el diálogo entre las aplicaciones de los sistemas finales. Los servicios de esta capa pueden ser prescindibles en algunos casos y en otros son obligatorios. Servicios de la capa sesión: control del diálogo, agrupamiento y recuperación.

- **RPC:** permite a un programa de ordenador ejecutar código en otra máquina remota sin tener que preocuparse por las comunicaciones entre ambos. Muy utilizadas para el modelo cliente-servidor.

- **SCP (Secure Copy):** a diferencia del RPC, los datos son cifrados durante su transferencia, para evitar que potenciales capturadores de paquetes (sniffers) extraigan información de los paquetes de datos.

- **ASP (Protocolo de sesión APPLE TALK):** de Apple, ofrece establecimiento de la sesión, mantenimiento y desmontaje, así como la secuencia petición.

Protocolos de Capa de Presentación (Capa 6 – Representación de la información): esta capa se tratan aspectos semánticos y sintácticos de los datos transmitidos. Se asegura de que, aunque distintos equipos puedan tener diferentes representaciones de caracteres ASCII, Unicode, EBCDIC, little-endian, big-endian, imágenes o sonidos, los datos lleguen de manera reconocible. Sus funciones son: formateo, cifrado y compresión de datos.

Protocolos de Capa de Aplicación (Capa 7 – Procesos de red a aplicaciones):

- **Hypertext Transfer Protocol (HTTP):** permite la comunicación adecuada entre navegadores y servidores web. Los navegadores web lo utilizan para solicitar archivos HTML de parte de los servidores remotos. Este protocolo tiene como base a TCP con modelo cliente-servidor y utiliza mensajes, algunos de ellos son:

§ **HTTP GET:** se envía información al servidor que contiene una URL y éste retorna una página WEB al navegador.

§ **HTTP POST:** se envía un mensaje al servidor que contiene los datos de la sección <body>, y así evitar envíos de información a través de la propia URL como sucede con HTTP GET.

§ **HTTP HEAD:** este mensaje restringe la respuesta del servidor, retornando solamente la información de la cabecera.

- **HTTPS** (Hypertext Transfer Protocol Secure) Protocolo seguro de transferencia de hipertexto.

- **FTP** (File Transfer Protocol - Protocolo de transferencia de archivos) para transferencia de archivos.

- **DNS** (Domain Name System - Sistema de nombres de dominio).

- **DHCP** (Dynamic Host Configuration Protocol - Protocolo de configuración dinámica de anfitrión).

- **POP** (Post Office Protocol) para recuperación de [correo electrónico].

- **SMTP** (Simple Mail Transport Protocol) para envío de correo electrónico.

- **SSH** (Secure SHell)

- **TELNET** para acceder a equipos remotos.

- **TFTP** (Trivial File Transfer Protocol).

- **LDAP** (Lightweight Directory Access Protocol).

- **XMPP** (Extensible Messaging and Presence Protocol) - Protocolo

1.4. DEFINA Y DESCRIBA MODELO OSI.

El modelo **OSI (Open System Interconnection)** es un modelo de referencia para los protocolos de la red. En este modelo hay siete capas, cada una de las cuales proporciona funciones de red específicas. Dividiendo la comunicación de red en partes más pequeñas y sencillas, además de normalizar los componentes de red para permitir el desarrollo y soporte de los productos de diferentes fabricantes.

Capa	Referencia	Funciones
7	La capa de aplicación	Procesos de red a aplicaciones
6	La capa de presentación	Representación de datos
5	La capa de sesión	Comunicación entres hosts
4	La capa de transporte	Conexiones de extremo a extremo
3	La capa de red	Direccionamiento y mejor ruta
2	La capa de enlace de datos	Acceso a los medios
1	La capa física	Transmisión binaria

Nro. Grupo:2

Encapsulamiento: Los datos viajan a través de las distintas capas, desde la capa de aplicación (más cercana al usuario) hasta la capa física (mecánica-eléctrica). Los pasos que se suceden son: Crear los datos, empaquetar los datos para ser transportados,

agregar dirección de red al encabezado, agregar dirección local al encabezado de enlace de datos y realizar la conversión a bits para su transmisión.

1.5. DEFINA TIPOS DE REDES SEGÚN:

1.6. EXTENSIÓN

1.6.1. LAN

Las redes **LAN** o redes de **área local** proporcionan acceso a terminales en un área geográfica pequeña o reducida. Las topologías físicas más utilizadas son: bus, anillo, estrella, estrella extendida, jerárquica, malla, árbol, doble anillo y mixta. En cuanto a las lógicas, las más utilizadas son: broadcast y tokens.

Los componentes de estas redes son:

- **Servidor:** equipos los cuales compartirán sus recursos hardware o software con los otros equipos de la red.
- **Estación de trabajo:** equipos que utilizan los recursos de la red y servidores.
- **Gateways:** hardware y software que permite las comunicaciones entre la red local y mainframes.
- **Bridges:** hardware y software que permite la conexión entre redes locales.
- **Tarjeta de red (NIC – Network Interface Card):** intermediaria entre el equipo y la red. En ella están los protocolos de comunicación.
- **El medio:** cables y conectores.

1.6.2. MAN

Las redes **MAN** o redes de **área metropolitana** proporcionan acceso a terminales en un área geográfica extensa. Es una colección de LANs dispersadas en una ciudad, con tiempos de acceso a la red mínimos para aplicaciones en tiempo real, aun cuando la carga de red sea elevada. Medios de transmisión: fibra óptica o par trenzado.

Fibra óptica: Ofrece un medio de transferencia de datos seguro ya que no es posible

leer o cambiar la señal óptica sin interrumpir físicamente el enlace.

Nodos de la red MAN: Las redes MAN pueden ser privadas o públicas, permitiendo la ejecución de más de 600 nodos, un gran número de puestos de trabajo.

Extensión de una red MAN: La extensión de la red puede ser de hasta 50km, dependiendo de la tecnología usada y de la infraestructura. La distancia permitida entre los nodos de acceso es de hasta 100 kilómetros, suficientes para conectar edificios de un área metropolitana.

Algunas redes **MAN** más utilizadas en la actualidad son: **Bonding EFM, SMDS y ATM.**

1.6.3. WAN

Las redes **WAN** o redes de **área amplia** es una red que une varias locales, especialmente construidas por organizaciones o empresas para su uso privado, o bien para uso público operadas por proveedores de internet para brindar conexión a sus clientes. Las redes **WAN** no conectan equipos sino redes enteras (**LAN**) pudiendo cubrir distancias entre 100km y 1.000 km, permitiendo conectar ciudad y países enteros. Permite comunicación en tiempo real y brindar recursos remotos a tiempo completo.

La infraestructura utilizada es la de **cableado estructurado**: cables, conectores, canalizadores y dispositivos.

Existen tres tipos de redes WAN:

- **Por circuitos:** son aquellas en las que se establece un canal dedicado entre los nodos y las terminales antes de que los usuarios se puedan comunicar. Ejemplo: redes de marcación (dial-up), redes de telefonía básica (RTB) y RDSI.

- **Por mensajes:** son equipos que aceptan el tráfico de cada terminal que se encuentre conectado a ella. Éstos pueden almacenar direcciones de mensajes, borrar, redirigir y responder mensajes en forma automática.
- **Por paquetes:** se dividen los mensajes en paquetes y se vuelven a unir cuando llegan a destino reconstruyendo el mensaje original. Facilita la corrección de errores y ayuda a aliviar el tráfico de datos. El ancho de banda es compartido entre todos los usuarios de la red.

1.7. FUNCIÓN.

1.7.1. SERVIDOR. PEER TO PEER?

1.7.2. CLIENTE – SERVIDOR.

Es una red de comunicaciones donde todos los clientes están conectados a un servidor, donde están centralizados los recursos de hardware y software a su disposición. Los roles se encuentran bien definidos, existiendo únicamente cliente o servidor, no pudiendo cambiar el rol en ningún momento.

Centralización del control: el servidor controla los recursos y la integridad de los datos.

Escalabilidad: Se pueden añadir tanto clientes como servidores, mejorarlos o añadir nodos a la red.

Encapsulación: a la hora de distribuir las funciones y responsabilidades entre varios equipos, es posible cambiar, reparar o actualizar un servidor sin que los clientes se vean afectados.

Tráfico: en este tipo de redes, el tráfico puede ser un problema, ya que cuando un servidor recibe una gran cantidad de peticiones el servidor puede presentar problemas.

Poca robustez: cuando el servidor se cae, los clientes no tienen acceso a los recursos.

Hardware y software dedicados: para este tipo de redes, es necesario que el servidor posea hardware y software dedicados, aumentando costos

1.8. CONEXIÓN FÍSICA.

Una red tiene dos tipos de conexiones: conexiones físicas que permiten a los ordenadores transmitir y recibir señales directamente y conexiones lógicas, o virtuales, que permiten intercambiar información a las aplicaciones informáticas, por ejemplo, a un procesador de textos. Las conexiones físicas están definidas por el medio empleado para transmitir la señal, por la disposición geométrica de los ordenadores (topología), por el método usado para compartir información, identifica cómo se interconectan los dispositivos finales y de infraestructura, como los routers, los switches y los puntos de acceso inalámbrico.

1.8.1. INALÁMBRICA.

Nro. Grupo:2

Se comunica a través de cables de datos (generalmente basada en Ethernet). Los cables de datos, conocidos como cables de red de Ethernet o cables con hilos conductores, conectan computadoras y otros dispositivos que forman las redes. Las redes alámbricas son mejores cuando se necesita mover grandes cantidades de datos a altas velocidades, como medios multimedia de calidad profesional.

Ventajas:

- Costos relativamente bajos
- Ofrece el máximo rendimiento posible
- Mayor velocidad

Desventajas:

- El costo de instalación siempre ha sido un problema muy común en este tipo de

tecnología, ya que el estudio de instalación, las canaletas, conectores, cables y otros no mencionados suman costos muy elevados en algunas ocasiones.

- El acceso físico es uno de los problemas más comunes dentro de las redes alámbricas, ya que, para llegar a ciertos lugares, es muy complicado el paso de los cables a través de las paredes de concreto u otros obstáculos.
- Dificultad y expectativas de expansión es otro de los problemas más comunes, ya que cuando pensamos tener un número definido de nodos, la mayoría del tiempo hay necesidades de construir uno nuevo y ya no tenemos espacio en los switches instalados.

1.8.1.1. PAR TRENZADO

Nro. Grupo:2

El cable de par trenzado consiste en grupos de hilos de cobre entrelazados en pares en forma helicoidal. Esto se hace porque dos alambres paralelos constituyen una antena simple. Cuando se entrelazan los alambres helicoidalmente, las ondas se cancelan, por lo que la interferencia producida por los mismos es reducida lo que permite una mejor transmisión de datos.

Así, la forma entrelazada permite reducir la interferencia eléctrica tanto exterior como de pares cercanos y permite transmitir datos de forma más fiable. Un cable de par trenzado está formado por un grupo de pares entrelazados (normalmente 2, 4 o 25 pares), recubiertos por un material aislante. Cada uno de estos pares se identifica mediante un color.

Está limitado en distancia, ancho de banda y tasa de datos. También destacar que la atenuación es una función fuertemente dependiente de la frecuencia. La interferencia y el ruido externo también son factores importantes, por eso se utilizan coberturas externas y el trenzado. Para señales analógicas se requieren amplificadores cada 5 o 6 kilómetros, para señales digitales cada 2 o 3. En transmisiones de señales analógicas punto a punto, el ancho de banda puede llegar hasta 250 kHz. En transmisión de señales digitales a larga distancia, la velocidad de datos no es demasiado grande, no

es muy efectivo para estas aplicaciones o dispositivos. En redes locales que soportan ordenadores locales, la velocidad de datos puede llegar a 10 Mbps (Ethernet) y 100 Mbps (Fast Ethernet).

En el cable par trenzado de cuatro pares, normalmente solo se utilizan dos pares de conductores, uno para recibir (cables 3 y 4) y otro para transmitir (cables 1 y 2), aunque no se pueden hacer las dos cosas a la vez, teniendo una transmisión half-dúplex. Si se utilizan los cuatro pares de conductores la transmisión es full-dúplex.

Tipos de cable par trenzado:

UTP (Unshielded Twisted Pair o Cable trenzado sin apantallar): Son cables de pares trenzados sin apantallar que se utilizan para diferentes tecnologías de red local. Son de bajo costo y de fácil uso, pero producen más errores que otros tipos de cable y tienen limitaciones para trabajar a grandes distancias sin regeneración de la señal.

STP (Shielded Twisted Pair o Par trenzado apantallado): Se trata de cables de cobre aislados dentro de una cubierta protectora, con un número específico de trenzas por pie. STP se refiere a la cantidad de aislamiento alrededor de un conjunto de cables y, por lo tanto, a su inmunidad al ruido. Se utiliza en redes de ordenadores como Ethernet o Token Ring. Es más caro que la versión no apantallada o UTP.

FTP (Foiled Twisted Pair o Par trenzado con pantalla global): Contiene pares trenzados, todos rodeados de una cubierta protectora hecha de aluminio. Es similar al caso anterior pero este último es más utilizado en equipos inalámbricos en exteriores. su impedancia característica es de 120 ohmios.

Tipos de conexión:

Los cables UTP forman los segmentos de Ethernet y pueden ser cables rectos o cables cruzados dependiendo de su utilización.

- **Cable recto** (pin a pin): Estos cables conectan un concentrador a un nodo de red (Hub, Nodo). Cada extremo debe seguir la misma norma (EIA/TIA 568A o 568B) de configuración. La razón es que el concentrador es el que realiza el cruce de la señal.
- **Cable cruzado** (cross-over): Este tipo de cable se utiliza cuando se conectan elementos del mismo tipo, dos enrutadores, dos concentradores. También se utiliza cuando conectamos 2 ordenadores directamente, sin que haya enrutadores o algún elemento de por medio.

Para hacer un cable cruzado se usará una de las normas en uno de los extremos del cable y la otra norma en el otro extremo.

Ventajas:

Nro. Grupo:2

- Bajo costo en su contratación.
- Alto número de estaciones de trabajo por segmento.
- Facilidad para el rendimiento y la solución de problemas.
- Puede estar previamente cableado en un lugar o en cualquier parte.

Desventajas:

- Altas tasas de error a altas velocidades.
- Ancho de banda limitado.
- Baja inmunidad al ruido.
- Alto coste de los equipos.
- Distancia limitada (100 metros por segmento).

1.8.1.2. CABLE COAXIAL

El cable coaxial es un cable utilizado para transportar señales eléctricas de alta frecuencia que posee dos conductores concéntricos, uno central, llamado núcleo, encargado de llevar la información, y uno exterior, de aspecto tubular, llamado malla, blindaje o trenza, que sirve como referencia de tierra y retorno de las corrientes. Entre ambos se encuentra una capa aislante dieléctrica, de cuyas características dependerá principalmente la calidad del cable. Todo el conjunto suele estar protegido por una cubierta aislante.

El conductor central puede estar constituido por un alambre sólido o por varios hilos retorcidos de cobre; mientras que el exterior puede ser una malla trenzada, una lámina enrollada o un tubo corrugado de cobre o aluminio. En este último caso resultará un cable semirrígido.

La característica importante del cable coaxial consiste en que es una estructura blindada. El campo electromagnético asociado con cada unidad coaxial está limitado nominalmente al espacio entre los conductores interior y exterior. Puesto que, al aumentar la frecuencia, la corriente alterna se concentra en el interior del conductor externo (efecto pelicular), una unidad coaxial es una línea de transmisión auto blindada, cuyo blindaje se mejora a frecuencias más altas. Las líneas no blindadas, tales como los pares de cable multipar, comparten el espacio para los campos electromagnéticos. Entonces, para una pérdida equivalente de transmisión, los pares ocupan menor espacio que los coaxiales. El uso principal del cable coaxial es la transmisión de señales de alta frecuencia de banda ancha. Los cables coaxiales se usan poco, o cerca de la frecuencia de voz dado que las propiedades de blindaje son pobres, además de que son más caros que los pares trenzados, con la misma pérdida de transmisión.

Para transmisión de portadora transcontinental, se usa mucho una variación del cable semirrígido, aislado con discos de polietileno dentro de un tubo de cobre. La unidad coaxial aislada con discos tiene pérdida muy baja, y actualmente se usa en sistemas de portadora en Estados Unidos, Japón y Europa, para transmitir hasta 10 800 canales bidireccionales de frecuencia de voz, por cada par de unidades coaxiales.

Tipos de cable coaxial:

Existen múltiples tipos de cable coaxial, cada uno con un diámetro e impedancia diferentes. El cable coaxial no es habitualmente afectado por interferencias externas, y es capaz de lograr altas velocidades de transmisión en largas distancias. Por esa razón, se utiliza en redes de comunicación de banda ancha (cable de televisión) y cables de banda base (Ethernet).

El tipo de cable que se debe utilizar depende de la ubicación del cable. Los cables coaxiales pueden ser de dos tipos:

- **Cloruro de polivinilo (PVC):** es un tipo de plástico utilizado para construir el aislante y la cubierta protectora del cable en la mayoría de los tipos de cable coaxial. El de PVC es flexible y se puede instalar fácilmente en cualquier lugar. Sin embargo, cuando se quema, desprende gases tóxicos.

Nro. Grupo:2

- **Plenum:** contiene materiales especiales en su aislamiento y en una clavija del cable. Estos materiales son resistentes al fuego y producen una mínima cantidad de humo tóxico. Sin embargo, el cableado plenum es más caro y menos flexible que el PVC.

1.8.1.3. FIBRA ÓPTICA

La fibra óptica es una fibra flexible, transparente, hecha al embutir o extruir vidrio (sílice) o plástico en un diámetro ligeramente más grueso que el de un cabello humano. Las fibras ópticas se utilizan más comúnmente como un medio para transmitir luz entre dos puntas de una fibra y tienen un amplio uso en las comunicaciones por fibra óptica, donde permiten la transmisión en distancias y en un ancho de banda (velocidad de datos) más grandes que los cables eléctricos. Se usan fibras en vez de alambres de metal porque las señales viajan a través de ellas con menos pérdida; además, las fibras son inmunes a la interferencia electromagnética, un problema del cual los cables de metal sufren ampliamente. Las fibras también se usan para la iluminación e imagería, y normalmente se envuelven en paquetes para introducir o sacar luz de

espacios reducidos, como en el caso de un fibroscopio. Algunas fibras diseñadas de manera especial se usan también para una amplia variedad de aplicaciones diversas, algunas de ellas son los sensores de fibra óptica y los láseres de fibra.

Tipos de fibra óptica:

Las diferentes trayectorias que puede seguir un haz de luz en el interior de una fibra se denominan modos de propagación. Y según el modo de propagación tendremos dos tipos de fibra óptica: multimodo y monomodo.

- **Fibra multimodo:** Una fibra multimodo es aquella en la que los haces de luz pueden circular por más de un modo o camino. Esto supone que no llegan todos a la vez. Una fibra multimodo puede tener más de mil modos de propagación de luz. Las fibras multimodo se usan comúnmente en aplicaciones de corta distancia, menores a 2 km, es simple de diseñar y económico.

El núcleo de una fibra multimodo tiene un índice de refracción superior, pero del mismo orden de magnitud, que el revestimiento. Debido al gran tamaño del núcleo de una fibra multimodo, es más fácil de conectar y tiene una mayor tolerancia a componentes de menor precisión.

Dependiendo el tipo de índice de refracción del núcleo, tenemos dos tipos de fibra multimodo:

- **Índice escalonado:** en este tipo de fibra, el núcleo tiene un índice de refracción constante en toda la sección cilíndrica, tiene alta dispersión modal.
- **Índice gradual:** mientras en este tipo, el índice de refracción no es constante, tiene menor dispersión modal y el núcleo se constituye de distintos materiales.
- **Fibra monomodo:** Una fibra monomodo es una fibra óptica en la que solo se propaga un modo de luz. Se logra reduciendo el diámetro del núcleo de la fibra hasta un tamaño (8,3 a 10 micrones) que solo permite un modo de propagación. Su transmisión es paralela al eje de la fibra. A diferencia de las fibras multimodo, las fibras

monomodo permiten alcanzar grandes distancias (hasta 400 km máximo, mediante un láser de alta intensidad) y transmitir elevadas tasas de información (10 Gbit/s).

Tipos según su diseño:

De acuerdo a su diseño, existen dos tipos de cable de fibra óptica

- **Cable de estructura holgada:** Es un cable empleado tanto para exteriores como para interiores que consta de varios tubos de fibra rodeando un miembro central de refuerzo y provisto de una cubierta protectora. Cada tubo de fibra, de dos a tres milímetros de diámetro, lleva varias fibras ópticas que descansan holgadamente en él. Los tubos pueden ser huecos o estar llenos de un gel hidrófugo que actúa como protector antihumedad impidiendo que el agua entre en la fibra. El tubo holgado aísla la fibra de las fuerzas mecánicas exteriores que se ejerzan sobre el cable.

Su núcleo se complementa con un elemento que le brinda resistencia a la tracción que bien puede ser de varilla flexible metálica o dieléctrica como elemento central o de hilaturas de Aramida o fibra de vidrio situadas periféricamente.

- **Cable de estructura ajustada:** Es un cable diseñado para instalaciones en el interior de los edificios, es más flexible y con un radio de curvatura más pequeño que el que tienen los cables de estructura holgada.

Contiene varias fibras con protección secundaria que rodean un miembro central de tracción, todo ello cubierto de una protección exterior. Cada fibra tiene una protección plástica extrusionada directamente sobre ella, hasta alcanzar un diámetro de 900 μm rodeando al recubrimiento de 250 μm de la fibra óptica. Esta protección plástica además de servir como protección adicional frente al entorno, también provee un soporte físico que serviría para reducir su coste de instalación al permitir reducir las bandejas de empalmes.

Ventajas:

- Una banda de paso muy ancha, lo que permite flujos muy elevados (del orden del GHz).
- Gran ligereza, el peso es del orden de algunos gramos por kilómetro, lo que resulta unas nueve veces menos que el de un cable convencional.
- Inmunidad total a las perturbaciones de origen electromagnético, lo que implica una calidad de transmisión muy buena, ya que la señal es inmune a las tormentas, chisporroteo, entre otros.
- Gran seguridad: la intrusión en una fibra óptica es fácilmente detectable por el debilitamiento de la energía lumínica en recepción, además, no irradia nada, lo que es particularmente interesante para aplicaciones que requieren alto nivel de confidencialidad.
Nro. Grupo:2
- No produce interferencias.
- Insensibilidad a las señales parásitas, lo que es una propiedad principalmente utilizada en los medios industriales fuertemente perturbados (por ejemplo, en los túneles del metro). Esta propiedad también permite la coexistencia por los mismos conductos de cables ópticos no metálicos con los cables de energía eléctrica.
- Atenuación muy pequeña independiente de la frecuencia, lo que permite salvar distancias importantes sin elementos activos intermedios. Puede proporcionar comunicaciones hasta 70 km antes de que sea necesario regenerar la señal, además, puede extenderse a 150 km utilizando amplificadores láser.
- Gran resistencia mecánica, lo que facilita la instalación.
- Resistencia al calor, frío y corrosión.
- Facilidad para localizar los cortes gracias a un proceso basado en la reflectometría, lo que permite detectar rápidamente el lugar donde se hará la reparación de la avería, simplificando la labor de mantenimiento.

Desventajas:

A pesar de las ventajas antes enumeradas, la fibra óptica presenta una serie de desventajas frente a otros medios de transmisión, siendo las más relevantes las siguientes:

- La alta fragilidad de las fibras.
- Necesidad de usar transmisores y receptores más costosos.
- Los empalmes entre fibras son difíciles de realizar, especialmente en el campo, lo que dificulta las reparaciones en caso de ruptura del cable.
- No puede transmitir electricidad para alimentar repetidores intermedios.
- La necesidad de efectuar, en muchos casos, procesos de conversión eléctrica-
Nro. Grupo:2
óptica.
- La fibra óptica convencional no puede transmitir potencias elevadas.
- La fibra óptica no transmite energía eléctrica, esto limita su aplicación donde el terminal de recepción debe ser energizado desde una línea eléctrica. La energía debe proveerse por conductores separados.
- Las moléculas de hidrógeno pueden difundirse en las fibras de silicio y producir cambios en la atenuación. El agua corroe la superficie del vidrio y resulta ser el mecanismo más importante para el envejecimiento de la fibra óptica.

1.8.1.4. HUB - SWITCH - ACCESS POINT

HUB

Es un dispositivo que permite centralizar el cableado de una red de computadoras, para luego poder ampliarla.

Trabaja en la capa física (capa 1) del modelo OSI o la capa de acceso al medio en el

modelo TCP/IP. Esto significa que dicho dispositivo recibe una señal y repite esta señal emitiéndose por sus diferentes puertos (repetidor).

En la actualidad, la tarea de los concentradores la realizan, con frecuencia, los conmutadores (switches).

SWITCH

Conmutador (switch) es el dispositivo digital lógico de interconexión de equipos que opera en la capa de enlace de datos del modelo OSI. Su función es interconectar dos o más host de manera similar a los puentes de red, pasando datos de un segmento a otro de acuerdo con la dirección MAC de destino de las tramas en la red y eliminando la conexión una vez finalizada esta.

Nro. Grupo:2

Los conmutadores se utilizan cuando se desea conectar múltiples tramos de una red, fusionándose en una sola red. Al igual que los puentes, dado que funcionan como un filtro en la red y solo transmiten la información hacia los tramos en los que hay el destinatario de la trama de red, mejoran el rendimiento y la seguridad de las redes de área local (LAN).

Clasificación:

Atendiendo al método de direccionamiento de las tramas utilizadas

- **Store-and-Forward:** Los conmutadores Store-and-Forward guardan cada trama en un búfer antes del intercambio de información hacia el puerto de salida. Mientras la trama está en el búfer, el switch calcula el CRC y mide el tamaño de la misma. Si el CRC falla, o el tamaño es muy pequeño o muy grande (una trama Ethernet tiene entre 64 bytes y 1518 bytes) la trama es descartada. Si todo se encuentra en orden es encaminada hacia el puerto de salida.
- **Cut-Through:** Los conmutadores cut-through fueron diseñados para reducir esta

latencia. Esos switches minimizan el delay leyendo sólo los 6 primeros bytes de datos de la trama, que contiene la dirección de destino MAC, e inmediatamente la encaminan.

- **Adaptive Cut-Through:** Son los conmutadores que procesan tramas en el modo adaptativo y son compatibles tanto con store-and-forward como con cut-through. Cualquiera de los modos puede ser activado por el administrador de la red, o el switch puede ser lo bastante inteligente como para escoger entre los dos métodos, basado en el número de tramas con error que pasan por los puertos.

Cuando el número de tramas corruptas alcanza un cierto nivel, el conmutador puede cambiar del modo cut-through a store-and-forward, volviendo al modo anterior cuando la red se normalice.

Nro. Grupo:2

Atendiendo a la forma de segmentación de las subredes

- **Conmutadores de capa 2:** Son los conmutadores tradicionales, que funcionan como puentes multi-puertos. Su principal finalidad es dividir una LAN en múltiples dominios de colisión, o en los casos de las redes en anillo, segmentar la LAN en diversos anillos. Basan su decisión de envío en la dirección MAC destino que contiene cada trama.

Los conmutadores de la capa 2 posibilitan múltiples transmisiones simultáneas sin interferir en otras sub-redes. Los switches de capa 2 no consiguen, sin embargo, filtrar difusiones o broadcasts, multicasts (en el caso en que más de una subred contenga las estaciones pertenecientes al grupo multicast de destino), ni tramas cuyo destino aún no haya sido incluido en la tabla de direccionamiento.

- **Conmutadores de capa 3:** Son los conmutadores que, además de las funciones tradicionales de la capa 2, incorporan algunas funciones de enrutamiento o routing, como por ejemplo la determinación del camino basado en informaciones de capa de red (capa 3 del modelo OSI), validación de la integridad del cableado de la capa 3 por checksum y soporte a los protocolos de routing tradicionales (RIP, OSPF,

etc)

Los conmutadores de capa 3 soportan también la definición de redes virtuales (VLAN), y según modelos posibilitan la comunicación entre las diversas VLAN sin la necesidad de utilizar un router externo.

ACCESS POINT

Un punto de acceso inalámbrico (en inglés: wireless access point, conocido por las siglas WAP o AP), en una red de computadoras, es un dispositivo de red que interconecta equipos de comunicación inalámbricos, para formar una red inalámbrica que interconecta dispositivos móviles o tarjetas de red inalámbricas.

Son dispositivos que son configurados en redes de tipo inalámbricas que son intermediarios entre una computadora y una red (Internet o local). Facilitan conectar varias máquinas cliente sin la necesidad de un cable (mayor portabilidad del equipo) y que estas posean una conexión sin limitar tanto su ancho de banda.

Los WAP son dispositivos que permiten la conexión de un dispositivo móvil de cómputo (computadora, tableta, smartphone) con una red. Normalmente, un WAP también puede conectarse a una red cableada, y puede transmitir datos entre los dispositivos conectados a la red cableada y los dispositivos inalámbricos.

Los WAP tienen asignadas direcciones IP, para poder ser configurados.

1.8.1.5. ROUTER

Un router es un dispositivo que permite interconectar computadoras que funcionan en el marco de una red. Se encarga de establecer la ruta que se destinará a cada paquete de datos dentro de una red informática.

El funcionamiento básico de un enrutador o encaminador, como se deduce de su nombre, consiste en enviar los paquetes de red por el camino o ruta más adecuada en

cada momento. Para ello almacena los paquetes recibidos y procesa la información de origen y destino que poseen. Con arreglo a esta información reenvía los paquetes a otro encaminador o bien al anfitrión final, en una actividad que se denomina 'encaminamiento'. Cada encaminador se encarga de decidir el siguiente salto en función de su tabla de reenvío o tabla de encaminamiento, la cual se genera mediante protocolos que deciden cuál es el camino más adecuado o corto, como protocolos basado en el algoritmo de Dijkstra.

Por ser los elementos que forman la capa de red, tienen que encargarse de cumplir las dos tareas principales asignadas a la misma:

- Reenvío de paquetes: cuando un paquete llega al enlace de entrada de un encaminador, este tiene que pasar el paquete al enlace de salida apropiado. Una característica importante de los encaminadores es que no difunden tráfico difusivo.
- Encaminamiento de paquetes: mediante el uso de algoritmos de encaminamiento tiene que ser capaz de determinar la ruta que deben seguir los paquetes a medida que fluyen de un emisor a un receptor.

Por tanto, debemos distinguir entre reenvío y encaminamiento. Reenvío consiste en coger un paquete en la entrada y enviarlo por la salida que indica la tabla, mientras que por encaminamiento se entiende el proceso de hacer esa tabla.

1.8.2. INALÁMBRICA (BLUETOOTH-WIFI)

Conjunto de computadoras, o de cualquier dispositivo informático comunicados entre sí mediante soluciones que no requieran el uso de cables de interconexión.

Ventajas:

- Flexibilidad: Dentro de la zona de cobertura de la red inalámbrica los nodos se podrán comunicar y no estarán atados a un cable para poder estar comunicados por el mundo.
- Poca planificación: Con respecto a las redes cableadas. Antes de cablear un edificio o unas oficinas se debe pensar mucho sobre la distribución física de las máquinas, mientras que con una red inalámbrica sólo nos tenemos que preocupar de que el edificio o las oficinas queden dentro del ámbito de cobertura de la red.
- Diseño: Los receptores son bastante pequeños y pueden integrarse dentro de un dispositivo y llevarlo en un bolsillo, etc.

Desventajas:

Nro. Grupo:2

- Menor ancho de banda: Las redes de cable actuales trabajan a 100 Mbps, mientras que las redes inalámbricas Wi-Fi lo hacen a 11 Mbps. Existen estándares que alcanzan los 54 Mbps y soluciones propietarias que llegan a 100 Mbps, pero estos estándares están en los comienzos de su comercialización y tiene un precio superior al de los actuales equipos Wi-Fi.
- Mayor inversión inicial: Para la mayoría de las configuraciones de la red local, el coste de los equipos de red inalámbricos es superior al de los equipos de red cableada.
- Seguridad: Las redes inalámbricas tienen la particularidad de no necesitar un medio físico para funcionar. Esto fundamentalmente es una ventaja, pero se convierte en una desventaja cuando se piensa que cualquier persona con una computadora portátil solo necesita estar dentro del área de cobertura de la red para poder intentar acceder a ella. Como el área de cobertura no está definida por paredes o por ningún otro medio físico, a los posibles intrusos no les hace falta estar dentro de un edificio o estar conectado a un cable.
- Interferencias: Las redes inalámbricas funcionan utilizando el medio radio electrónico en la banda de 2,4 GAZ. Esta banda de frecuencias no requiere de licencia

administrativa para ser utilizada por lo que muchos equipos del mercado, como teléfonos inalámbricos, microondas, etc., utilizan esta misma banda de frecuencias. Además, todas las redes Wi-Fi funcionan en la misma banda de frecuencias incluida la de los vecinos. Este hecho hace que no se tenga la garantía de que nuestro entorno radioelectrónico esté completamente limpio para que nuestra red inalámbrica funcione a su más alto rendimiento. Cuanto mayores sean las interferencias producidas por otros equipos, menor será el rendimiento de nuestra red.

1.8.2.1. TOPOLOGÍA

La topología de red se define como el mapa físico o lógico de una red para intercambiar datos. En otras palabras, es la forma en que está diseñada la red, sea en el plano físico o lógico. El concepto de red puede definirse como «conjunto de ^{oro. de po. 2} nodos interconectados». Un nodo es el punto en el que una curva se intercepta a sí misma. Lo que un nodo es concretamente depende del tipo de red en cuestión.

La topología de red determina únicamente la configuración de las conexiones entre nodos. La distancia entre los nodos, las interconexiones físicas, las tasas de transmisión y los tipos de señales no pertenecen a la topología de la red, aunque pueden verse afectados por la misma.

Tipos de topología:

Los estudios de topología de red reconocen ocho tipos básicos de topologías:

- Punto a punto (point to point, PtP) o peer-to-peer (P2P)
- En bus (“conductor común” o bus) o lineal (line)
- En estrella (star)
- En anillo (ring) o circular
- En malla (mesh)

- En árbol (tree) o jerárquica
- Topología híbrida, combinada o mixta, por ej. circular de estrella, bus de estrella
- Cadena margarita (daisy chain)

1.8.2.2. BUS, TRONCAL

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

Es la tercera de las topologías principales. Las estaciones están conectadas por un único segmento de cable. A diferencia de una red en anillo, el bus es pasivo, no se produce generación de señales en cada nodo o router. En la topología de bus, todos los nodos (computadoras) están conectados a un circuito común (bus). La información que se envía de una computadora a otra viaja directamente o indirectamente, si existe un controlador que enruta los datos al destino correcto. La información viaja por el cable en ambos sentidos a una velocidad aproximada de 10/100 Mbps y tiene en sus dos extremos una resistencia (terminador). Se pueden conectar una gran cantidad de computadoras al bus, si un computador falla, la comunicación se mantiene, no sucede lo mismo si el bus es el que falla. El tipo de cableado que se usa puede ser coaxial, par trenzado o fibra óptica. En una topología de bus, cada computadora está conectada a un segmento común de cable de red. El segmento de red se coloca como un bus lineal, es decir un cable largo que va de un extremo a otro de la red, y al cual se conecta cada nodo de ésta. El cable puede ir por el piso, las paredes, el techo o por varios lugares, siempre y cuando sea un segmento continuo.

Ventajas:

- Facilidad de implementación y crecimiento.

- Fácil adaptación.
- Simplicidad en la arquitectura.
- Es una red que no ocupa mucho espacio.

Desventajas:

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

Nro. Grupo:2

1.8.2.3. ESTRELLA

Una red en estrella es una red de computadoras donde las estaciones están conectadas directamente a un punto central y todas las comunicaciones se hacen necesariamente a través de ese punto (conmutador, repetidor o concentrador). Los dispositivos no están directamente conectados entre sí, además de que no se permite tanto tráfico de información. Dada su transmisión, una red en estrella activa tiene un nodo central “activo” que normalmente tiene los medios para prevenir problemas relacionados con el eco.

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

paquetes de usuarios.

Ventajas:

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

Nro. Grupo:2

Desventajas:

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

1.8.2.4. ESTRELLA, TRONCAL

Una red troncal (o network backbone) es la parte de la infraestructura de red informática que interconecta diferentes redes, lo que les permite comunicarse entre sí, y proporciona una ruta para el intercambio de datos entre estas diferentes redes.

Las redes discretas tienen varias formas de “hablar” entre sí. Si tiene dos redes separadas, digamos entre dos ubicaciones de “Puntos de presencia” (PoP, point of presence), pueden enviar tráfico a través de Internet pública, establecer túneles encriptados a través de Internet pública o conectarse a través de un circuito físico dedicado que solo se conecta entre ellos.

Las redes troncales conectan redes de área local (LAN) y redes de área amplia (WAN) juntas. Las redes troncales de red están diseñadas para maximizar la confiabilidad y el rendimiento de las comunicaciones de datos a gran escala y a larga distancia.

1.9. COMUNICACIÓN(PROTOCOLOS)

El objetivo principal de todo sistema de comunicaciones es intercambiar información entre dos entidades. La siguiente figura muestra un ejemplo particular de comunicación entre una estación de trabajo y un servidor a través de una red telefónica pública.

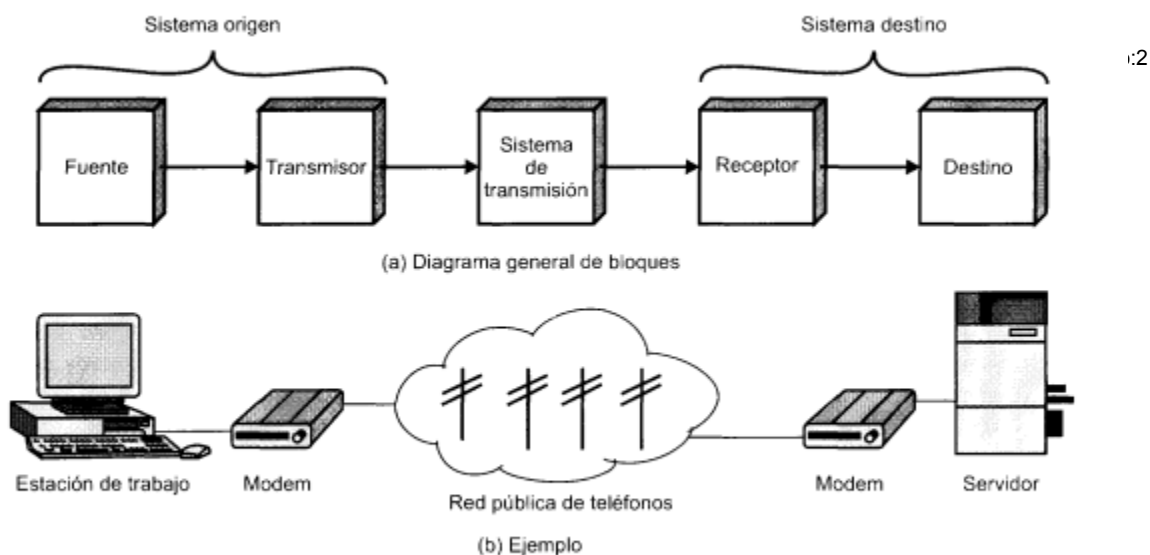


Figura 1.1. Modelo simplificado para las comunicaciones.

Los elementos clave en este modelo son los siguientes:

- **La fuente.** Este dispositivo genera los datos a transmitir: por ejemplo teléfonos o computadores personales.
- **El transmisor.** Normalmente los datos generados por la fuente no se transmiten

directamente tal y como son generados. Al contrario, el transmisor transforma y codifica la información. generando señales electromagnéticas susceptibles de ser transmitidas a través de algún sistema de transmisión. Por ejemplo, un modem convierte las cadenas de bits generadas por un computador personal y las transforma en señales analógicas que pueden ser transmitidas a través de la red telefónica.

- **El sistema de transmisión**, que puede ser desde una sencilla línea de transmisión hasta una compleja red que conecte a la fuente con el destino.
- **El receptor**, que acepta la señal proveniente del sistema de transmisión y la transforma de tal manera que pueda ser manejada por el dispositivo destino. Por ejemplo, un modem captará la señal analógica de la red o línea de transmisión y la convertirá en una cadena de bits.

Nro. Grupo:2

- **El destino**, que toma los datos del rector.

Aunque el modelo presentado pueda parecer aparentemente sencillo, en realidad implica una gran complejidad. Para hacerse una idea de la magnitud de ella, la Tabla 1.1 lista algunas de las tareas claves que se deben realizar en un sistema de comunicaciones. Esta relación es en un sentido un tanto arbitraria

Tabla 1.1. Tareas en los sistemas de comunicación.

Utilización del sistema de transmisión Implementación de la interfaz Generación de la señal Sincronización Gestión del intercambio Detección y corrección de errores Control de flujo	Direccionamiento Encaminamiento Recuperación Formato de mensajes Seguridad Gestión de red
---	--

El primer ítem **utilización del sistema de transmisión** se refiere a la necesidad de hacer un uso eficaz de los recursos utilizados en la transmisión, los cuales típicamente se suelen compartir entre una serie de dispositivos de comunicación. La capacidad total del medio de transmisión se reparte entre los distintos usuarios haciendo uso de técnicas denominada de multiplexación. Además, puede que se necesiten técnicas de control de congestión para garantizar que el sistema no se sature por una demanda excesiva de servicios de transmisión.

Para que un dispositivo pueda transmitir información tendrá que hacerlo a través de la **Interface el medio de transmisión**, cuando la interfaz está establecida, se necesitara la generación de la **señal**. Las características de la señal, tales como la forma y la intensidad. deben ser tales que permitan: 1) Ser propagadas a través ^{Nro. Grupo:2} del medio de transmisión y 2) ser interpretada en el receptor como datos.

Las señales se deben generar no sólo considerando que deben cumplir los requisitos del sistema de transmisión y del receptor, sino que deben permitir alguna forma de **sincronizar** el receptor y el emisor. El **receptor** debe ser capaz de determinar cuándo comienza y cuando acaba la señal recibida. Igualmente, deberá conocer la duración de cada elemento de señal.

Además de las cuestiones básicas referentes a la naturaleza y temporización de las señales, se necesitará verificar un conjunto de requisitos que pueden englobar bajo el término de **gestión de intercambio**. Si necesita intercambiar datos durante un periodo de tiempo, las dos partes deben cooperar ejemplo, para los dos elementos que intervienen en una conversación telefónica (emisor y receptor), uno de ellos debe marcar el número del otro, dando lugar a una serie de señales especiales que harán que el otro Teléfono suene. En este ejemplo el receptor establece la llamada descolgando el auricular. En dispositivos para el procesamiento de datos, se necesitan

ciertas convenciones además del simple hecho de establecer conexión

Por ejemplo, se deberá establecer si ambos dispositivos pueden transmitir simultáneamente o deben hacerlo por turnos, se deberá decidir la cantidad y el formato de los datos que se transmiten cada vez, y se debe especificar qué hacer en caso de que se den ciertas contingencias, como por ejemplo la detección de un error.

Los dos ítems siguientes (Tabla 1.1) deberían considerarse dentro de la gestión del intercambio, pero debido a su importancia, se consideran por separado. En todos los sistemas de comunicación es posible que **aparezcan errores**: es decir, la señal transmitida se distorsiona de alguna manera antes de alcanzar su destino. Por tanto, en circunstancias donde no se puedan tolerar errores, se necesitarán ^{Nro. Grupo:2} **procedimientos para la detección y corrección de errores**. Así, por ejemplo, en sistemas para el procesamiento de datos, si se transfiere un fichero desde un computador a otro, no sería aceptable que el contenido del fichero se modificara accidentalmente. Para evitar que la fuente no sature al destino transmitiendo datos más rápidamente de lo que el receptor pueda procesar y absorber, se necesitan una serie de procedimientos denominados **control de flujo**.

Conceptos relacionados pero distintos a los anteriores son el **direccionamiento** y el **encaminamiento**. Cuando cierto recurso se comparte por más de dos dispositivos, el sistema fuente deberá de alguna manera indicar a dicho recurso compartido la identidad del destino. El sistema de transmisión deberá garantizar que ese destino, y sólo éste, reciba los datos. Es más, el sistema de transmisión puede ser una red en la que exista la posibilidad de más de un camino para alcanzar al destino, en este caso se necesitará, por tanto, la elección de una de entre las posibles rutas.

La **recuperación** es un concepto distinto a la corrección de errores. En ciertas

situaciones en las que el intercambio de información, por ejemplo, una transacción de una base de datos o la transferencia de un fichero, se vea interrumpida por algún fallo, se necesitará un mecanismo de recuperación. El objetivo será pues, o bien ser capaz de continuar transmitiendo desde donde se produjo la interrupción, o al menos recuperar el estado donde se encontraban los sistemas involucrados antes de comenzar el intercambio.

El **formato de mensajes** está relacionado con el acuerdo que debe existir entre las dos partes respecto al formato de los datos intercambiados, como por ejemplo el código binario usado para representar los caracteres.

Además, frecuentemente es necesario dotar al sistema de algunas ^{Nro. Grupo:2}medidas de **seguridad**. El emisor debe asegurarse de que sólo el destino deseado reciba los datos. Igualmente, el receptor querrá estar seguro de que los datos recibidos no se han alterado en la transmisión y que dichos datos realmente provienen del supuesto emisor.

Por último, todo el sistema de comunicación es lo suficientemente complejo como para ser diseñado y utilizado sin más, es decir, se necesita la habilidad de un **gestor de red** que configure el sistema, monitorice su estado, reaccione ante fallos y sobrecargas, y planifique con acierto los crecimientos futuros.

COMUNICACIONES DE DATOS

La Figura 1.2 muestra una perspectiva del modelo tradicional para las comunicaciones, el ejemplo es una aplicación de correo electrónico

Suponiendo que tanto el dispositivo de entrada como el transmisor están en un computador personal. Y que por ejemplo, el usuario de dicho PC desea enviar el mensaje m a otro. El usuario activa la aplicación de correo en el PC y compone el mensaje con el teclado (**dispositivo de entrada**). La cadena de caracteres se almacena temporalmente en la memoria principal como una secuencia de **bits (g)**. El computador se conecta a algún medio de transmisión, por ejemplo, una red local o una línea telefónica, a través de un dispositivo de E/S (transmisor), como por ejemplo el <<transceiver>> a una red local o modem. Los datos de entrada se transfieren al transmisor como una secuencia de niveles de tensión que representan los bits en algún tipo de bus de comunicaciones o cable. El transmisor se conecta directamente al medio y convierte la cadena en la señal a transmitir .

Nro. Grupo:2

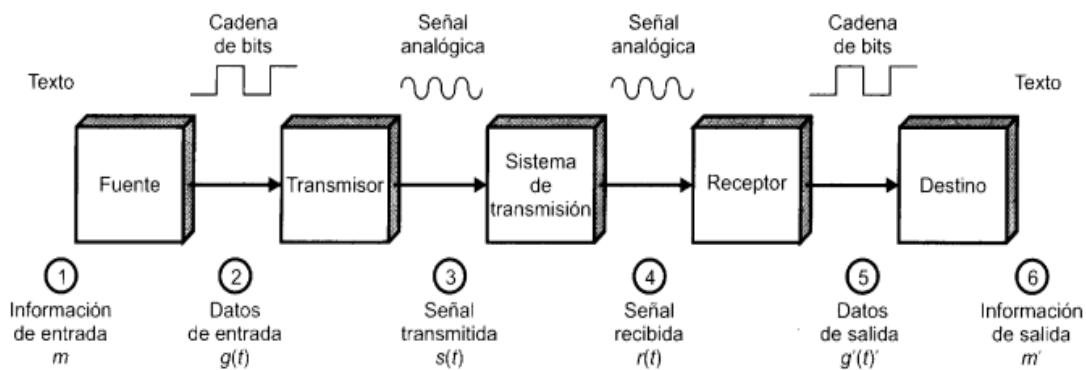


Figura 1.2. Modelo simplificado para las comunicaciones de datos.

Al transmitir a través del medio, antes de llegar al receptor, aparecerán una serie de dificultades. Por lo tanto, la señal recibida $r(t)$ puede diferir de alguna manera de la transmitida $s(t)$. El receptor intentará estimar la señal original $s(t)$, a partir de la señal $r(t)$ y de su conocimiento acerca del medio, obteniendo una secuencia de bits $g'(t)$

Estos bits se envían al computador de salida, donde se almacenan temporalmente en memoria como un bloque de bits (g'). En muchos casos, el destino intentará determinar si ha ocurrido un error, y en su caso, cooperar con el origen para eventualmente conseguir el bloque de datos completo y sin errores. Los datos, finalmente se presentan al usuario a través del dispositivo de salida, que por ejemplo puede ser la impresora o la pantalla de su terminal. El mensaje recibido por el usuario (m') será normalmente una copia exacta del mensaje original (m).

En el anterior ejemplo no se han considerado otros aspectos fundamentales en las comunicaciones de datos, como lo son las técnicas de control del enlace, necesarias para regular el flujo de información, o como la detección y corrección de errores, tampoco se han considerado las técnicas de multiplexación, necesarias para conseguir una utilización eficaz del medio de transmisión.

Nro. Grupo:2

PROTOCOLOS Y ARQUITECTURA DE PROCOLOS

Cuando se realiza un intercambio de datos entre computadores, terminales y/o otros dispositivos se debe considerar otros procedimientos, por ejemplo, la transferencia de un fichero entre dos computadores. En este caso, debe haber un camino entre los dos computadores, **directo** o a través de **una red de comunicación**, pero de más, típicamente se requiere la realización de las siguientes tareas adicionales:

1. El sistema fuente de información debe activar el camino directo de datos, o bien debe proporcionar a la red de comunicación la identificación del sistema destino deseado.
2. El sistema fuente debe asegurarse de que el destino está preparado para recibir datos.
3. La aplicación de transferencia de fichero en el origen debe asegurarse de que el programa gestor en el destino está preparado para aceptar y almacenar el fichero para el usuario determinado,

4. Si los formatos de los dos ficheros son incompatibles entre ambos sistemas, uno de los dos deberá realizar una operación de adecuación.

Al intercambio de información entre computadores con el propósito de cooperare le denomina **comunicación entre computadores**. De igual manera, al conjunto de computadores que se interconectan a través de una red de comunicaciones, se les denomina **red de computadores**. Estos términos se extienden igualmente a cuando alguna de las partes es un terminal, ya que el grado de cooperación en este caso es similar.

En el estudio de las comunicaciones entre computadores y las redes de computadores, son especialmente relevantes los dos conceptos siguientes

Nro. Grupo:2

- Los protocolos.
- Las arquitecturas para comunicaciones entre computadores

Para la comunicación entre dos entidades situadas en sistemas diferentes es necesario la definición y utilización de un protocolo.

Antes que los términos entidad-sistema se están usando muy general Ejemplos entidades son: los programas de aplicación de los usuarios, las utilidades para transferencias de ficheros, los sistemas de gestión de base de datos, así como los gestores de correo electrónico y terminales.

Ejemplos de sistemas son: los computadores, los terminales y los sensores remotos.

Para que dos entidades se comuniquen con éxitos, se requiere que «**hablen el mismo idioma**». Qué se comunica, cómo se comunica. y cuándo se comunica debe seguir una

serie de convenciones mutuamente aceptadas por las entidades involucradas. Este conjunto de convenios se denominan **protocolos**, que se pueden definir como el conjunto de reglas que gobiernan el intercambio de datos entre dos entidades. Los puntos clave que definen o caracterizan a un protocolo son:

- **La sintaxis:** incluye aspectos tales como el formato de los datos y los niveles de señal.
- **La semántica:** incluye información de control para la coordinación y el manejo de errores.
- **La temporización:** incluye la sintonización de velocidades y secuenciación.

Nro. Grupo:2

Un protocolo de red es un conjunto de reglas que realiza la comunicación de datos a través de una red a fin de llevar a cabo diferentes transacciones.

También conocido como **protocolo de comunicación**, el protocolo de red establece la semántica y la sintaxis del intercambio de información, algo que constituye un estándar. Las computadoras en red, de este modo, tienen que actuar de acuerdo a los parámetros y los criterios establecidos por el protocolo en cuestión para lograr comunicarse entre sí y para recuperar datos que, por algún motivo, no hayan llegado a destino.

En el protocolo de red se incluyen diversas informaciones que son imprescindibles para la conexión. **El protocolo indica** cómo se concreta la conexión física, establece la manera en que debe comenzar y terminar la comunicación, determina cómo actuar ante datos corrompidos, protege la información ante el ataque de intrusos, señala el eventual cierre de la transmisión, etc.

Por ejemplo, está el Protocolo de Control de Transmisión/Protocolo Internet (TCP/IP) define un conjunto de reglas que se utilizan en el envío de datos de un nodo a otro de

la red.

El Protocolo Simple de Transferencia de Correo (SMTP) es un conjunto de reglas y estándares que se utilizan para la transferencia de correo electrónico y archivos adjuntos de un nodo a otro.

El Protocolo dinámico de configuración de anfitrión (DHCP) es un protocolo —un conjunto de reglas y estándares— que se utiliza para asignar, de manera dinámica, direcciones IP en una red, a fin de que no sea necesario asignarlas a cada estación de trabajo en forma manual.

En la conectividad de redes se utilizan muchos protocolos. En realidad, en cierto sentido, casi todas las actividades en una red están regidas por un protocolo de un tipo o de otro. Algunos protocolos funcionan en niveles bajos del modelo de red OSI, otros ^{Nro. Grupo: 2} trabajan en niveles altos y algunos más trabajan entre éstos.

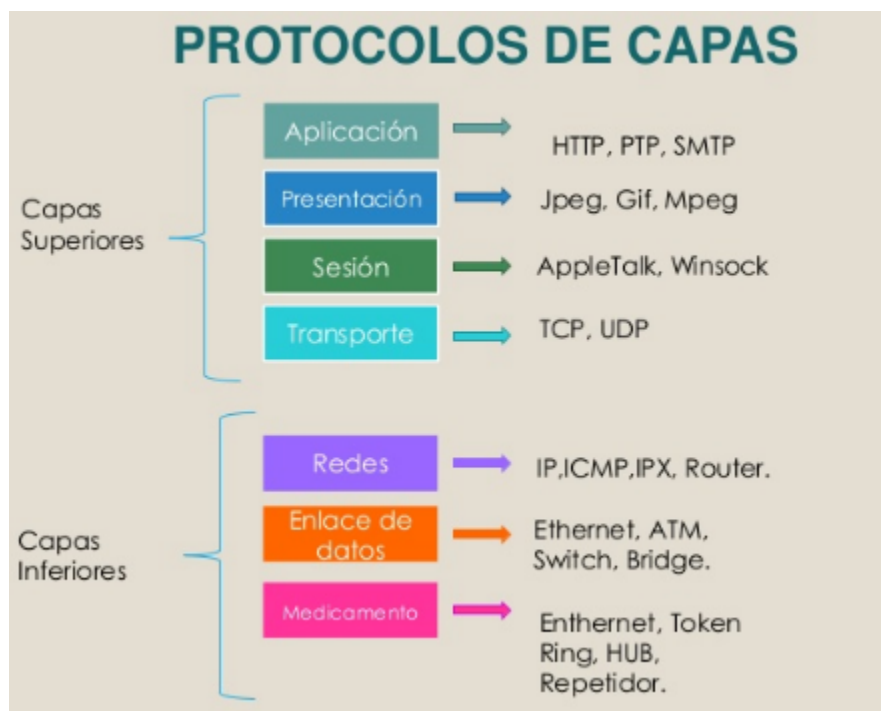
Un protocolo debe llevar a cabo las siguientes funciones:

1. Lograr la atención de las otras partes en la comunicación.
2. Identificar el componente con los otros componentes en la comunicación.
3. Proporcionar un indicar constante de que los datos están siendo recibidos y comprendidos, o bien sea todo lo contrario.
4. Solicitar la retransmisión de los datos erróneos.
5. Iniciar el procedimiento de recuperación si aparecen datos.
6. Proporcionar una forma aceptable de concluir una transmisión para garantizar que todas las partes han terminado.

Tipos de Protocolos de Red

- **Protocolo asíncrono:** en esta transmisión los datos se transmite un carácter a la vez, usando bits de inicio y final.
- **Protocolo síncrono:** esta transmisión es continua. Las terminales transmisoras receptoras deben sincronizarse, es decir estar en fase entre sí.
- **Transmisión Half-Duplex:** La transmisión de los datos se produce en un solo sentido a la vez. Si está recibiendo datos no se puede transmitir.
- **Transmisión Full-Duplex:** la transmisión de los datos se produce en ambos sentidos al mismo tiempo un extremo que está recibiendo datos puede, al mismo tiempo, estar transmitiendo otros datos.

Nro. Grupo:2



1.9.1. TCP/IP (TRANSFER CONTROL PROTOCOL/INTERNET PROTOCOL)

COMPRENSIÓN DE TCP Y UDP

TCP/IP son en realidad dos protocolos que se utilizan en concierto uno con el otro. El **Protocolo Internet (IP)** define cómo se direccionan los datos de la red desde una fuente hacia un destino y qué secuencia de datos debe reensamblarse en el otro extremo. El protocolo IP trabaja en la capa de red del modelo OSI. El **Protocolo de control de la transmisión (TCP)** es un protocolo de alto nivel que trabaja una capa más arriba que el IP, en la capa de transporte.

TCP administra las conexiones entre computadoras. Los mensajes TCP son transportados (encapsulados) en **datagramas IP**.

El Protocolo de datagrama de usuario (UDP) sirve para el mismo propósito que TCP, pero ofrece un menor número de características. Tanto los paquetes TCP como los UDP son transportados dentro de paquetes IP, pero la única característica de confiabilidad que soporta UDP es el reenvío de cualquier número de paquetes que no se reciban en el destino. (El protocolo UDP es no orientado a la conexión.) La **ventaja primordial** del UDP es que es más rápido en comunicaciones de red triviales, como el envío de páginas web a una computadora cliente.

Puertos TCP y UDP

Tanto TCP como UDP soportan el concepto de **puertos, o de direcciones específicas de aplicación**, con la ayuda de las cuales los paquetes se envían a cualquier máquina receptora. Por ejemplo, la mayoría de los servidores web corren en una computadora tipo servidor y reciben paquetes a través del puerto número 80. Cuando una máquina recibe un paquete que está destinado al servidor web (como una solicitud de una página web), la computadora que lo solicita envía esos paquetes al puerto con ese número. Cuando usted solicita una página web del servidor, su computadora

envía la solicitud a la computadora servidora y especifica que su solicitud debe enviarse al puerto 80, que es adonde se envían las solicitudes HTTP. Cientos de puertos diferentes tienen usos estandarizados y es fácil definir sus propios puertos en

un servidor para aplicaciones específicas.

Un archivo de texto llamado SERVICES define los puertos de una computadora. A continuación, se muestra un ejemplo de una parte del archivo SERVICES de Windows NT.

```
# Copyright (c) 1993-1999 Microsoft Corp.
#
# This file contains port numbers for well-known
# services as defined by
# RFC 1700 (Assigned Numbers).
#
# Format:
#
# <service name><port number>/<protocol>[aliases...][#<comment>]
#
echo                7/tcp
echo                7/udp
discard             9/tcp    sink null
discard             9/udp    sink null
sysstat             11/tcp    users        #Active users
daytime             13/tcp
daytime             13/udp
chargen             19/tcp    ttytst source #Character generator
chargen             19/udp    ttytst source #Character generator
ftp-data            20/tcp
ftp                 21/tcp    #FTP. control
telnet              23/tcp
smtp                25/tcp    mail         #SMTP
time                37/tcp    timserver
time                37/udp    timserver
```

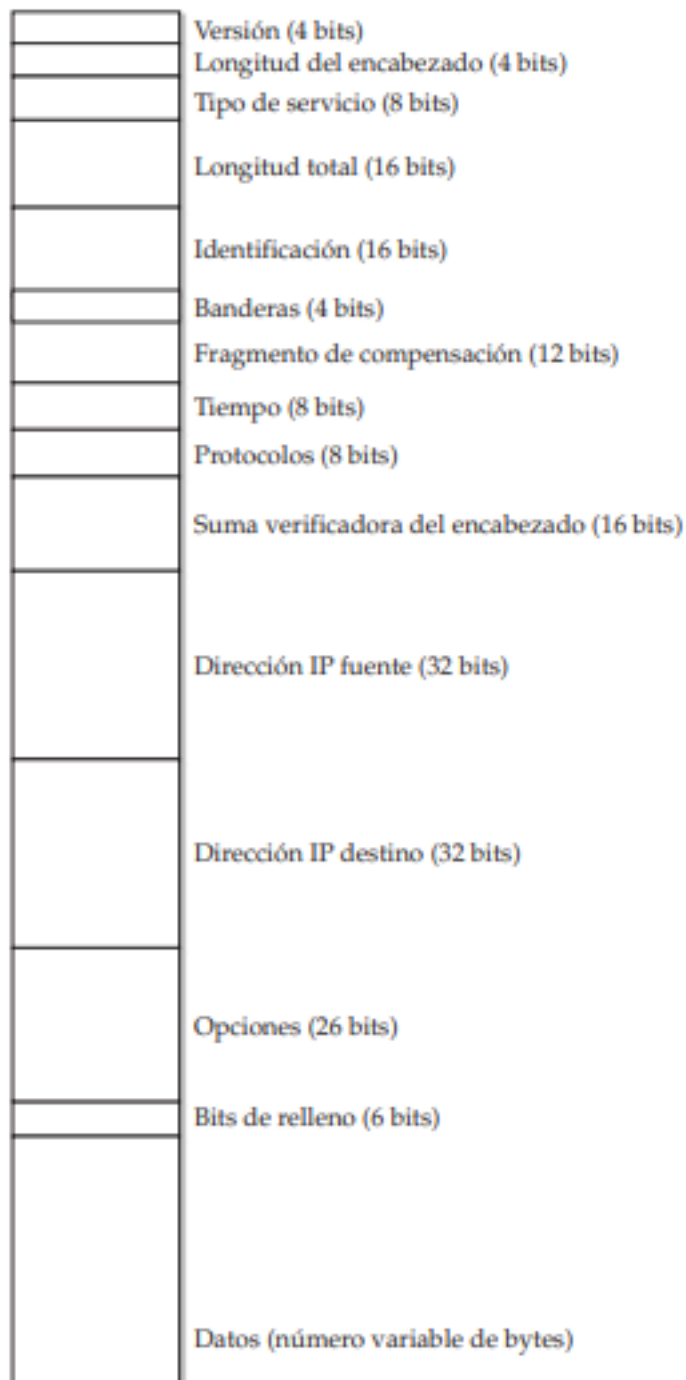
Nro. Grupo:2

El uso de puertos asegura que las comunicaciones de red que se desean utilizar para un propósito en particular no se confundan con otras que puedan estar llegando a la misma máquina. Los puertos permiten que la máquina receptora envíe, adecuadamente, los datos que están llegando a ella. Un ejemplo es un servidor que almacena páginas web y también recibe y procesa correo electrónico. Los paquetes que llegan al puerto 80 se enviarán al software servidor de red, mientras que los que lleguen al puerto 25 se enviarán al software de correo electrónico.

1.9.2. DEFINA QUE ES UNA IP

Internet Protocol, (Protocolo de Internet). Es el sistema estándar mediante el cual funciona la internet, por medio de un proceso de envío y recepción de información. Una dirección IP es un conjunto de números, únicos e irrepetibles, que identifica a un

dispositivo con la capacidad de conectarse a internet, ya sea una computadora, tableta, celular, o incluso dispositivos inteligentes preparados para IoT (Internet de las cosas). En los **paquetes IP se incluyen direcciones que definen, de manera única, cada computadora conectada a Internet** (Ver figura paquete IP).



Nro. Grupo:2

Estas direcciones se utilizan para **enrutar** paquetes de un nodo emisor a uno receptor. Debido a que todos los routers de Internet conocen las direcciones de red a las que están conectados, pueden enviar paquetes, de manera muy precisa, que tengan como destino una red remota.

Además de transportar sus datos, cada paquete IP contiene varios campos. Estos campos, en el orden en el que se encuentran, son:

- **Versión** Ésta es la versión del protocolo IP que se está utilizando. Indica, por ejemplo, si se está utilizando la versión 4 o la versión 6 de IP.
- **Longitud del encabezado** Este campo indica la longitud de la información del encabezado antes de que comiencen los datos que contiene el paquete.
- **Tipo de servicio** Este campo es utilizado para diferentes actividades por los diversos fabricantes. Puede utilizarse para funciones como solicitud de enrutamiento de alta prioridad, solicitud de envío con el más alto nivel de confiabilidad, etcétera.
- **Longitud total** Este campo indica la longitud total del paquete.
- **Identificación**, **banderas** y **fragmentos** fuera de su lugar Estos tres campos se utilizan para reensamblar cualquier paquete IP que haya sido desensamblado en algún punto durante la transmisión. Estos campos incluyen toda la información necesaria para reensamblar correctamente los paquetes en el extremo receptor.
- **Tiempo de vida** Este campo define cuántos saltos en la red puede realizar un paquete antes de que se le declare como muerto y los routers dejen de enviarlo a otros routers. Este número se establece cuando se envía el paquete y cada router que lo maneja decrementa dicho número una unidad. Cuando el número llega a un valor de cero, el paquete se considera muerto y ya no es transmitido.
- **Protocolo** Este campo indica si el paquete IP está contenido en un paquete

TCP o UDP.

- **Suma de verificación del encabezado** La suma verificadora del encabezado se utiliza para asegurarse de que ningún dato (los campos estudiados en esta lista) del encabezado del paquete resulte dañado.
- **Dirección IP fuente** Este campo contiene la dirección de la computadora emisora, la cual es necesaria cuando un paquete debe ser retransmitido, en cuyo caso el nodo receptor (o, en algunos casos, un ruteador) conoce a qué nodo solicitar una retransmisión.
- **Dirección IP destino** Este campo contiene la dirección del nodo receptor.
- **Opciones y relleno** Estos dos campos finales del encabezado del paquete IP se utilizan para solicitar cualquier instrucción acerca de algún enrutamiento específico que se requiera o para especificar el tiempo en el que se envió el paquete.
- **Datos** El campo final de un paquete IP son los datos que, en realidad, están siendo enviados.

Las direcciones **IP son de 32 bits de longitud**, lo que permite que el número máximo de direcciones sea de 2^{32} o aproximadamente 4.3 mil millones de direcciones. Para que sea más fácil trabajar con ellas y para enrutarlas de una manera más eficiente, se dividen en cuatro octetos, cada uno con una longitud de un byte. Por tanto, en notación decimal, las direcciones IP se expresan como xxx.xxx.xxx.xxx, donde cada xxx representa un número de 0 a 255. Los números 0, 127 y 255 están generalmente reservados para propósitos especiales, por lo que típicamente no se encuentran disponibles para los nodos, mientras que las 253 direcciones restantes están disponibles para asignarse en cada octeto.

Se garantiza que las direcciones en Internet sean únicas por medio del uso de un

servicio de registro de direcciones, que actualmente se encuentra administrado por la **Corporación de Internet para la Asignación de Nombres y Números** (ICANN). En realidad, los registros de los nombres y las direcciones de dominio están administrados mediante uno de los tantos registradores, los cuales incluyen compañías como INTERNIC, Network Solutions y muchas otras. El ICANN representa la autoridad máxima.

¿Cómo funciona una dirección IP?

El router es el que se encarga de asignar las IPs a los diferentes dispositivos que se van conectando. Gracias a esto es imposible que dos equipos tengan la misma IP. Por esta misma razón, no es posible mantener conexiones fijas entre varios dispositivos, como carpetas compartidas e impresoras. Puesto que cada vez que se ~~conecta~~ ^{se conectan} los equipos tendrán una IP diferente; esto es lo que sucede con las IPs dinámicas.

Si, en cambio, hablamos de una IP estática, como su nombre lo indica, estaríamos hablando de una dirección IP que no cambia, la cual sólo es posible haciendo una configuración en el dispositivo.

¿Cómo buscar la dirección IP de un sitio web?

1. Presiona el botón “Inicio” de tu computadora.
2. Escribe en el buscador de programas y archivos “cmd”.
3. Presiona “Enter”.
4. Se abrirá la consola MS-DOS, donde debes escribir “nslookup google.com”. En vez de “google.com”, debes escribir el nombre del dominio de la página que deseas consultar.

5. Enseguida, podrás ver la dirección IP.

TIPOS DE DIRECCIONES

- **Según su versión** pueden ser IPv4 o IPv6. Explico sus diferencias más abajo.
- **IP pública o privada.** Dependen del tipo de red a que pertenezcan.
- **IP fija o dinámica.** En función del modo en que se asignan.

1.9.3. DIFERENCIA IP ESTATICA Y DINAMICA

Nro. Grupo:2

Estáticas: Es la dirección IP asignada a un dispositivo, **la cual no cambia**. Es decir que utilizará el mismo número IP de por vida. Se aplica tanto para direcciones públicas o privadas. Las direcciones IP estáticas ofrecen **mayor estabilidad y velocidad de descarga**. Aunque, pueden ser más *vulnerables* a ciertos inconvenientes, como al ataque de hackers por ejemplo; ya que al ser direcciones estáticas, los hackers cuentan con más tiempo para operar en ellas. Para obtener una dirección IP es necesario pagar una cuota adicional y la configuración de estas debe ser de forma manual, así que si no tienes mucho conocimiento técnico será necesario contratar a alguien para que te ayude con el servicio.

Dinámicas: Se caracterizan por que **van cambiando cada vez que el dispositivo se conecta a Internet**. Se usa generalmente cuando los proveedores tienen más clientes que direcciones IP debido a la poca probabilidad que existe de que todos se conecten al mismo tiempo.

Además de ofrecer una mayor seguridad y privacidad, su configuración es automática. Sin embargo, un punto débil de este tipo de dirección IP, es la probabilidad de que la *conexión se interrumpa*, pues eso se sucede con más frecuencia que en una IP fija. Es por eso, que muchas veces cuando el modem que provee de Wifi en tu casa debe ser desconectado y conectado para mejorar la conexión, es decir, para cambiar de número IP.

1.9.4. DIFERENCIA IP RESERVADA (PRIVADA, PUBLICA)

IP Pública: Es la que tiene asignada cualquier equipo o dispositivo conectado de forma directa a Internet. Algunos ejemplos son: los servidores que alojan sitios web como Google, los router o modems que dan acceso a Internet, otros ^{Nro. Grupo?} elementos de hardware que forman parte de su infraestructura, etc. Las IP públicas **son siempre únicas**. No se pueden repetir. Dos equipos con IP de ese tipo pueden conectarse directamente entre sí. Por ejemplo, tu router con un servidor web. O dos servidores web entre sí.

IP Privada: Se utiliza para identificar equipos o dispositivos dentro de una red doméstica o privada. En general, en redes que no sean la propia Internet y utilicen su mismo protocolo (el mismo "idioma" de comunicación).

Las IP públicas y privadas no son diferentes en sí mismas, como tampoco lo son las IP fijas y dinámicas. **Tienen una forma y una función muy parecidas pero se utilizan en casos distintos.**

¿Cómo se usan en la práctica las IP privadas?

Al configurar una red en casa u oficina, esa red la componen un PC fijo, un laptop

portátil, una impresora y un router de acceso a Internet.

Cada elemento de la red tendrá su propia IP dentro de los rangos que has visto antes. Por ejemplo, 192.168.1.1 (el router), 192.168.1.2 (el PC fijo), 192.168.1.3 (el laptop) y 192.168.1.50 (la impresora en red).

Si se quiere ampliar la red, no tienes más que asignar otra IP al nuevo PC, la nueva impresora o los adaptadores de red adicionales que puedas instalar. Siempre en los rangos admitidos.

Estas IP deben ser únicas dentro de una misma red. Cada equipo o dispositivo ha de tener la suya, distinta de la de los demás. De lo contrario habría problemas.

Las IP privadas **sí pueden repetirse en redes distintas** (como en la tuya y la de una empresa). Los equipos o dispositivos con esas IP pueden conectarse entre sí SÓLO dentro de la red a que pertenecen. No hay conflictos porque las redes están separadas. Igual que no los hay entre dos direcciones físicas iguales de ciudades distintas.

Para conectar una red privada con Internet (u otra red) hace falta una especie de **traductor**. Es una función del router llamada **NAT, por las siglas de Network Address Translation (Traducción de Dirección de Red)**.

El NAT sirve de puente o intermediario. Permite cosas como poder entrar desde tu PC (que tiene una IP privada) en el servidor donde está un sitio web (que tiene una IP pública).

1.9.5. DIFERENCIA IPV4, IPV6

Hoy en día hay dos versiones en uso del protocolo IP. Eso hace que pueda tener aspectos y características distintos, estos son:

IPv4

Es la versión estándar. La usan la inmensa mayoría de los equipos y dispositivos de Internet y otras redes. Las IP de este tipo tienen una forma como esta: 212.150.67.158

Suele escribirse así por una cuestión práctica y de facilidad de lectura. Como cuatro números decimales, que pueden variar cada uno entre 0 y 255, separados por puntos.

Los equipos informáticos trabajan en realidad con bits. 1 bit puede tener sólo dos valores. O cero o uno. Los bits sirven para definir estados como encendido o apagado, verdadero o falso, más o menos, etc. Así funcionan internamente los equipos y sus programas. Cada número de la IPv4 representa 8 bits. O lo que es lo mismo, 1 byte. Por tanto sus direcciones están formadas en total por **32 bits o 4 bytes** (4 grupos de 8 bits cada uno, $4 \times 8 = 32$). Hay otra versión de IP que está en crecimiento y que es la alternativa del futuro. Se llama **IPv6**

IPv6

Surgió porque el IPv4 estaba "quedándose corto". Empezaban a acabarse las IP para identificar a los miles de millones de equipos y dispositivos de las redes mundiales e Internet.

¿Cuánto es eso en un número "normal"?

- Nº que permite el IPv6: 340.000.000.000.000.000.000.000.000.000.000.000.000

Nro. Grupo:2

Formas de escribir una IPv6

Hay más opciones que con la simple IPv4. Estas son las notaciones principales:

Notación completa

Tiene este aspecto:

2A03:2880:2110:CF01:0ACE:0000:0000:0009

128 bits).

Notación abreviada

Elimina los ceros que están al principio de cada grupo. Y representa con ":" el grupo o grupos consecutivos formado/s sólo por ceros.

La IPv6 anterior quedaría así (marco los cambios en negrita):\

2A03:2880:2110:CF01:**ACE::9**

En este ejemplo no se escriben los ceros que estaban al principio del quinto y octavo grupos. Y los ceros del sexto y séptimo grupo se han abreviado como ":".

Notación mixta

Nro. Grupo:2

Es la menos habitual. Escribe los últimos 32 bits con el formato del IPv4 y los demás con el del IPv6. Por ejemplo:

2A03:2880:2110:CF01:0ACE:0000:**212.150.67.158**

o bien

2A03:2880:2110:CF01:**ACE::212.150.67.158**

1.9.6. DEFINA CLASES DE DIRECCIONES IP (A, B, C, D, E)

Las direcciones IPv4, se encuentran agrupadas en 5 clases, las cuales, se identifican por el primer octeto de bits de la dirección IP.

¿Qué quiere decir el primer octeto de bits? las direcciones IP traducidas al código

binario, ocupan 32 bits, que son 32 unos o ceros.

1 st Octet	2 nd Octet	3 rd Octet	4 th Octet
\	\	/	/
11000000.10101000.00000001.10011000			
192	. 168	. 1	. 152

Entonces para diferenciar a que clase pertenece una dirección, miramos el primer octeto de bits.

El número de redes y la cantidad de hosts que puede manejar una IP por clase puede ser obtenida mediante esta fórmula:

Nro. Grupo:2

Número de redes	$=2^{\text{network_bits}}$
Número de Hosts/ redes	$=2^{\text{host_bits}}-2$

El primer bit del primer octeto siempre se establece en 0 (cero). Por lo tanto, el primer octeto varía de 1 - 127, es decir:

El primer número del octeto siempre permanece en 0, por lo tanto, hay 7 bits con los que combinar unos y ceros.

Ejemplo:

10.65.23.45 Es una dirección de clase A porque empieza por el número 10.

126.45.123.45 también lo es.

132.35.67.43 No es una dirección de clase A ya que no entra en el rango de 1-127. Es una dirección de clase B.

DIRECCIÓN DE CLASE A: puede albergar hasta 126 (27-2) redes y 16777214 (224-2) hosts (equipos).

00000001 - 01111111
1 - 127

Fíjate en las operaciones de arriba, 27 el número de combinaciones, uno o cero son dos, elevado a 7 por el número de bits disponibles del primer octeto (recuerda que el primer bit del octeto se queda siempre en cero), que es el que se utiliza en la clase A, por lo tanto 2.

Entonces 2 elevado a 7 son 128 direcciones de red posibles.

Nro. Grupo:2

Al calcular las direcciones IP hosts, 2 direcciones IP han disminuido debido a que no pueden ser asignados a los hosts, es decir, el primer IP de una red es número de red IP y la última es reservado para IP de difusión.

Así pues, nos quedan 126 direcciones de red asignables.

La siguiente operación (224-2), dos elevado a 24 bits reservados para hosts (los 3 octetos restantes de la dirección IP), menos dos, el número de red y la IP de difusión.

La máscara de subred determinada para la clase de dirección IP es 255.0.0.0.

Dirección IP de Clase A formato es así:

0NNNNNNN.HHHHHHHH.HHHHHHHH.HHHHHHHH

DIRECCIÓN DE CLASE B: la clase B tiene reservados los dos primeros bits del primer octeto, por lo tanto, sólo quedan 6 bits para hacer combinaciones.

10000000 – **10**111111
128 – 191

Direcciones IP de Clase B rango de 128.0 .x.x a 191.255 .x.x. La máscara de subred predeterminada de la Clase B es 255.255.x.x.

Clase B tiene 16384(2¹⁴) direcciones de red y 65534 (2¹⁶-2) direcciones de host.

Dirección IP de Clase B formato es:

10NNNNNN.NNNNNNNN.HHHHHHHH.HHHHHHHH

DIRECCIÓN DE CLASE C: El primer octeto de IP de Clase C tiene sus primeros 3 bits a 110, es decir:

11000000 – **110**11111
192 – 223

Las direcciones IP Clase C de 192.0.0.x a 192.255.255.x. La máscara de subred predeterminada de la Clase C es 255.255.255.x.

2097152 Da Clase C (2²¹) direcciones de red y 254 (2⁸-2) las direcciones de host.

Dirección IP de Clase C formato: 110NNNNN.NNNNNNNN.NNNNNNNN.HHHHHHHH

DIRECCIÓN DE CLASE D: se reservan los cuatro primeros bits del primer octeto:

11100000 – **1110**1111
224 – 239

La Clase D tiene la dirección IP 224.0.0.0 a 239.255.255.255, esta última dirección, es reservada para la **multidifusión**. Los datos de la multidifusión **no están destinados**

para un host en concreto, por eso no hay necesidad de extraer direcciones de host de la dirección IP, y la clase D **no tiene ninguna máscara de subred**.

DIRECCIÓN DE CLASE E:

Esta clase IP está reservada para fines experimentales. Las direcciones IP de esta clase van de 240.0.0.0 a 255.255.255.254 . Como la clase D, también esta clase no está equipada con máscara de subred.

1.9.7. CONCEPTO DNS (DOMAIN NAME SYSTEM)

El **Sistema de Nombres de Dominio** o DNS es un sistema de nomenclatura jerárquico que se ocupa de la **administración del espacio de nombres de dominio (Domain Name Space)**. Su labor primordial consiste en resolver las peticiones de asignación de nombres. Esta función se podría explicar mediante una comparación con un servicio telefónico de información que dispone de datos de contacto actuales y los facilita cuando alguien los solicita. Para ello, el sistema de nombres de dominio recurre a una red global de servidores DNS, que subdividen el espacio de nombres en zonas administradas de forma independiente las unas de las otras. Esto permite la gestión descentralizada de la información de los dominios.

Cada vez que un usuario registra un dominio, se crea una entrada **WHOIS** en el registro correspondiente y esta queda almacenada en el DNS como un “**resource record**”. La base de datos de un servidor DNS se convierte, así, en la compilación de todos los registros de la zona del espacio de nombres de dominio que gestiona.

El DNS (Sistema de Nombres de Dominio) es el encargado de “**traducir**” los **números de una dirección IP en un nombre de dominio**. Es decir que convierten el dominio

escrito en el navegador y dirigen el acceso hacia el servidor al que apunta el dominio.

1.9.8. CONCEPTO PUERTA DE ENLACE

La pasarela (en inglés **gateway**) o puerta de enlace es el dispositivo que actúa de interfaz de conexión entre aparatos o dispositivos, y también posibilita compartir recursos entre dos o más ordenadores.

Su propósito es traducir la información del protocolo utilizado en una red inicial, al protocolo usado en la red de destino.

Nro. Grupo:2

La pasarela es normalmente un equipo informático configurado para dotar a las máquinas de una red de área local (Local Area Network, LAN) conectadas a él de un acceso hacia una red exterior, generalmente realizando para ello operaciones de traducción de direcciones de red (Network Address Translation, NAT). Esta capacidad de traducción de direcciones permite aplicar una técnica llamada enmascaramiento de IP, usada muy a menudo para dar acceso a Internet a los equipos de una LAN compartiendo una única conexión a Internet, y por tanto, una única dirección IP externa.

La dirección IP de una pasarela a menudo se parece a 192.168.1.1 o 192.168.0.1 y utiliza algunos rangos predefinidos, 127.x.x.x, 10.x.x.x, 172.x.x.x, 192.x.x.x. Puedes averiguar la puerta de enlace de tu enrutador ejecutando el comando **ipconfig** desde el cmd de Windows, o ejecutando la orden **ip route** desde la terminal macOS o GNU/Linux.

Un equipo que haga de puerta de enlace en una red debe tener necesariamente dos tarjetas de red (Network Interface Card, NIC).

La puerta de enlace predeterminada (default gateway) es la ruta predeterminada o ruta por defecto que se le asigna a un equipo y tiene como función enviar cualquier paquete del que no conozca por cuál interfaz enviarlo y no esté definido en las rutas del equipo, enviando el paquete por la ruta predeterminada.

En entornos domésticos, se usan los routers ADSL como puertas de enlace para conectar la red local doméstica con Internet; aunque esta puerta de enlace no conecta dos redes con protocolos diferentes, sí que hace posible conectar dos redes independientes haciendo uso de NAT.

Nro. Grupo:2

1.9.9. CONCEPTO DHCP

DHCP significa **protocolo de configuración de host dinámico** y es un protocolo de red utilizado en redes IP donde un servidor DHCP asigna automáticamente una dirección IP y otra información a cada host en la red para que puedan comunicarse de manera eficiente con otros puntos finales.

Además de la *dirección IP*, **DHCP** también asigna la *máscara de subred*, la *dirección de puerta de enlace predeterminada*, la *dirección del servidor de nombres de dominio* (DNS) y otros parámetros de configuración pertinentes. La solicitud de comentarios (RFC) 2131 y 2132 define DHCP como un estándar definido por IETF (Internet Engineering Task Force) basado en el protocolo BOOTP. El protocolo de configuración de host dinámico simplifica y mejora la precisión del direccionamiento IP, pero puede generar inquietudes de seguridad.

1.9.10. CONCEPTO MASCARA DE SUBRED

Es la máscara de subred la que define qué parte de la dirección IP de la computadora es la netid y cuál el hostid. Para ver esto de una manera más clara, usted necesita representar las direcciones en forma binaria.

Computer IP Address (Dec):	205	143	60	109
Computer IP Address (Bin):	11001101	10001111	00111100	01101101
Subnet mask (Dec):	255	255	255	0
Subnet mask (Bin):	11111111	11111111	11111111	00000000

Nro. Grupo:2

La netid de una dirección, definida por la máscara de subred, es cualquier parte de la dirección que tenga un número binario 1 fijado en la máscara de subred correspondiente. En el ejemplo anterior, la netid está formada por los primeros tres octetos en su totalidad (los primeros 24 bits), y el hostid es el último octeto (los 8 últimos bits). Ahora puede ver por qué el 255 (decimal) se utiliza con tanta frecuencia en las máscaras de subred: es debido a que el 255 corresponde a tener todos los bits fijos al valor 1 en un número de 8 bits.

Imagínese que en casa se tiene un ordenador, una Xbox 360 conectada a Internet y un iPad. La IP del primero es 192.168.1.2, la del segundo 192.168.1.3 y la del tercero 192.168.1.4. Como podéis ver, los tres primeros números son iguales mientras que **el último cambia**. Pues es precisamente con la **máscara de subred como identificamos esa parte fija de la IP de la parte variable**. ¿Cómo? De una manera muy sencilla, marcando la parte que no varía con 255 y la parte que sí lo hace con 0. Así que, siguiendo el ejemplo anterior, la máscara de subred sería 255.255.255.0.

¿Y para qué sirve todo esto? Pues simplificando mucho, tienes que saber que las

partes fijas de tu IP representan la red que tienes para conectarte a Internet. Y la máscara de subred, que es el número que varía, se usa para que los ordenadores puedan determinar si las direcciones de los otros dispositivos con los que se quieren conectar están en la red local o la remota.

1.9.11. COMANDOS IP

CMD se puede definir que es un programa en modo de consola, parecido al famoso el intérprete de comandos de MSDOS, con la diferencia que alberga una gran cantidad de herramientas que nos permite interactuar tanto con el sistema operativo de nuestro equipo como con los equipos que están conectados a nuestra red.

Nro. Grupo:2

1.9.11.1. DESCRIBA IPCONFIG

El comando ipconfig es una forma rápida de determinar la dirección IP de su ordenador y otra información, como la dirección de su pasarela por defecto, útil si desea conocer la dirección IP de la interfaz web de su router.

```
Dirección física. . . . . : C0-38-96-0C-81-C9
DHCP habilitado . . . . . : sí
Configuración automática habilitada . . . : sí

Adaptador de LAN inalámbrica Wi-Fi:

Sufijo DNS específico para la conexión. . :
Descripción . . . . . : Realtek RTL8723BE Wireless LAN 80
2.11n PCI-E NIC
Dirección física. . . . . : C0-38-96-0C-81-C9
DHCP habilitado . . . . . : no
Configuración automática habilitada . . . : sí
Vínculo: dirección IPv6 local. . . . . : fe80::90c3:8f38:3b60:6def%4<Preferido>
Dirección IPv4. . . . . : 192.168.1.101<Preferido>
Máscara de subred . . . . . : 255.255.255.0
Puerta de enlace predeterminada . . . . . : 192.168.1.1
IAD DHCPv6 . . . . . : 146815126
DUID de cliente DHCPv6. . . . . : 00-01-00-01-1B-ED-A6-E6-F0-76-1C-
15-DE-20
Servidores DNS. . . . . : 80.58.61.250
80.58.61.254
NetBIOS sobre TCP/IP. . . . . : habilitado

Adaptador de Ethernet Ethernet:
```

Para usar el comando, simplemente escriba ipconfig en el símbolo del sistema. Verás una lista de todas las conexiones de red que utiliza el equipo. bajamos hasta donde

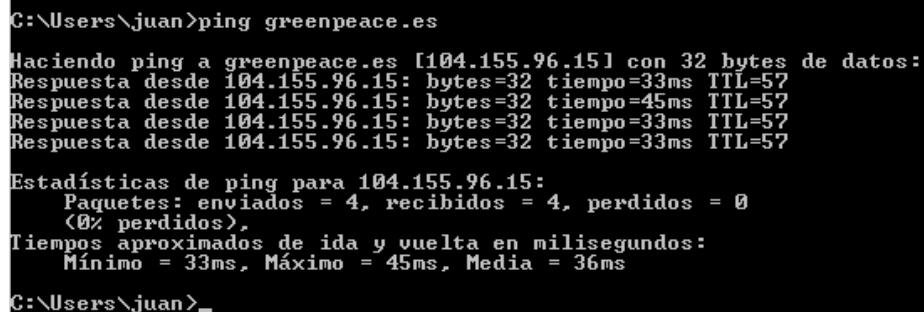
pone "Adaptador de LAN inalámbrica" para una conexión Wi-Fi o "Adaptador Ethernet" en caso de que estemos conectado por cable. Si se quiere más detalles, puedes usar el comando `ipconfig /all`.

1.9.11.2. DESCRIBA PING

Si tiene problemas de conexión a un sitio web u otros problemas de conexión de red, Windows y otros sistemas operativos tienen algunas herramientas estándar que puede usar para identificar problemas.

Primero, está el comando `ping`. Escriba **ping greenpeace.es** y Windows enviará paquetes a esa dirección.

Vemos el resultado en la siguiente imagen



```
C:\Users\juan>ping greenpeace.es

Haciendo ping a greenpeace.es [104.155.96.15] con 32 bytes de datos:
Respuesta desde 104.155.96.15: bytes=32 tiempo=33ms TTL=57
Respuesta desde 104.155.96.15: bytes=32 tiempo=45ms TTL=57
Respuesta desde 104.155.96.15: bytes=32 tiempo=33ms TTL=57
Respuesta desde 104.155.96.15: bytes=32 tiempo=33ms TTL=57

Estadísticas de ping para 104.155.96.15:
    Paquetes: enviados = 4, recibidos = 4, perdidos = 0
        (0% perdidos),
    Tiempos aproximados de ida y vuelta en milisegundos:
        Mínimo = 33ms, Máximo = 45ms, Media = 36ms

C:\Users\juan>_
```

Se puede hacer con el nombre del dominio o con la ip del servidor que acoge esta web (a fecha de hoy es 104.155.96.15

El servidor en esa dirección IP responderá y te hará saber que los ha recibido. Podrá ver si algún paquete no llegó al destino -quizás esté experimentando una pérdida de paquetes- y cuánto tiempo tardó en obtener la respuesta -quizás la red está saturada y los paquetes tardan un poco en llegar a su destino.

```
C:\Users\juan>tracert greenpeace.es

Trazo a la dirección greenpeace.es [104.155.96.151]
sobre un máximo de 30 saltos:

 1      1 ms      3 ms      1 ms      192.168.1.1
 2      13 ms     14 ms     13 ms     10.0.0.1
 3      14 ms     13 ms     14 ms     172.16.1.1
 4      14 ms     13 ms     65 ms     10.220.96.6
 5      14 ms     14 ms     14 ms     91.232.81.214
 6      13 ms     14 ms     14 ms     74.125.242.178
 7      29 ms     30 ms     29 ms     172.253.76.37
 8      34 ms     37 ms     35 ms     216.239.51.118
 9      33 ms     35 ms     40 ms     216.239.56.179
10      35 ms     34 ms     93 ms     108.170.235.53
11      *         *         *         Tiempo de espera agotado para esta solicitud.
12      *         *         *         Tiempo de espera agotado para esta solicitud.
13      *         *         *         Tiempo de espera agotado para esta solicitud.
14      *         *         *         Tiempo de espera agotado para esta solicitud.
15      *         *         *         Tiempo de espera agotado para esta solicitud.
16      *         *         *         Tiempo de espera agotado para esta solicitud.
17      *         *         *         Tiempo de espera agotado para esta solicitud.
18      *         *         *         Tiempo de espera agotado para esta solicitud.
19      *         *         *         Tiempo de espera agotado para esta solicitud.
20     34 ms     33 ms     33 ms     15.96.155.104.bc.googleusercontent.com [104.155.96.151]

Trazo completa.

C:\Users\juan>
```

o. Grupo:2

El comando Tracert rastrea la ruta que toma un paquete para llegar a un destino y le muestra información sobre cada salto a lo largo de esa ruta. Por ejemplo, si ejecuta greenpeace.es, verás información sobre cada nodo con el que el paquete interactúa en su camino hacia nuestro servidor. Si tiene problemas para conectarse a un sitio web, tracert puede mostrarle dónde está ocurriendo el problema.

En la imagen vemos que aparece en los tiempos el símbolo *. Esto significa que ese enrutador está configurado para no generar respuesta a las peticiones, pero funciona cuando se trata de enrutar paquetes de información tcp/ip.

2. MAQUINA VIRTUALES

2.1. DEFINICIÓN DE MÁQUINA VIRTUAL (VIRTUAL MACHINE)

Una máquina virtual (VM) es un software que simula un sistema de computación y puede ejecutar programas y aplicaciones como si fuese una computadora real. Una máquina virtual, generalmente conocida como invitado, se crea dentro de otro entorno informático denominado «host». Múltiples máquinas virtuales pueden existir dentro de un solo host a la vez.

Las máquinas virtuales se basan en arquitecturas de computadora y brindan la funcionalidad de una computadora física. Sus implementaciones pueden involucrar hardware especializado, software o una combinación.

Nro. Grupo:2

Una característica esencial de las máquinas virtuales es que los procesos que ejecutan están limitados por los recursos y abstracciones proporcionados por ellas. Estos procesos no pueden escaparse de esta "computadora virtual".

2.2. PARA QUE SIRVE UNA MAQUINA VIRTUAL

Uno de los usos domésticos más extendidos de las máquinas virtuales es ejecutar sistemas operativos para "probarlos". De esta forma podemos ejecutar un sistema operativo que queramos probar (GNU/Linux, por ejemplo) desde nuestro sistema operativo habitual (Mac OS X por ejemplo) sin necesidad de instalarlo directamente en nuestra computadora y sin miedo a que se desconfigure el sistema operativo primario.

También sirve para ejecutar alguna aplicación que corre exclusivamente en un SO desde otro. Un ejemplo muy común de hoy en día es el de los emulador del SO android ya sea desde Windows o iOS, así muchos pueden continuar el uso de aplicaciones que utilizan en su celular desde su ordenador.

2.3. TIPOS DE MÁQUINAS VIRTUALES

2.3.1. MÁQUINAS VIRTUALES DE SISTEMA

Las máquinas virtuales de sistema, también llamadas máquinas virtuales de hardware, permiten a la máquina física subyacente multiplicarse entre varias máquinas virtuales, cada una ejecutando su propio sistema operativo. A la capa de software que permite la virtualización se la llama monitor de máquina virtual o hypervisor. Un monitor de máquina virtual puede ejecutarse o bien directamente sobre el hardware o bien sobre un sistema operativo ("host operating system").

2.3.2. MÁQUINAS VIRTUALES DE PROCESO

Una máquina virtual de proceso, a veces llamada "máquina virtual de aplicación", se ejecuta como un proceso normal dentro de un sistema operativo y soporta un solo proceso. La máquina se inicia automáticamente cuando se lanza el proceso que se desea ejecutar y se detiene para cuando éste finaliza. Su objetivo es el de proporcionar un entorno de ejecución independiente de la plataforma de hardware y del sistema operativo, que oculte los detalles de la plataforma subyacente y permita que un programa se ejecute siempre de la misma forma sobre cualquier plataforma.

Entre las máquinas virtuales más utilizadas están:

- Oracle VM VirtualBox
- VMware Workstation

Oracle VM VirtualBox

Es un software de virtualización para arquitecturas x86/amd64, creado originalmente por la empresa alemana innotek GmbH. Actualmente es desarrollado por Oracle Corporation como parte de su familia de productos de virtualización. Por medio de esta aplicación es posible instalar sistemas operativos adicionales, conocidos como «sistemas invitados», dentro de otro sistema operativo «anfitrión», cada uno con su propio ambiente virtual.

Entre los sistemas operativos soportados (en modo anfitrión) se encuentran GNU/Linux, Mac OS X, OS/2 Warp, Microsoft Windows, y Solaris/OpenSolaris, y dentro de ellos es posible virtualizar los sistemas operativos FreeBSD, GNU/Linux, OpenBSD, OS/2 Warp, Windows, Solaris, MS-DOS y muchos otros.

VMware Workstation

[VMware](#) Inc., (VM de Virtual Machine) filial de EMC Corporation que proporciona la mayor parte del software de virtualización disponible para ordenadores compatibles X86. Entre este software se incluyen VMware Workstation, y los gratuitos VMware Server y VMware Player. El software de [VMware](#) puede funcionar en Windows, Linux, y en la plataforma Mac OS X que corre en procesadores INTEL, bajo el nombre de VMware Fusion.

Cuando se ejecuta el programa, proporciona un ambiente de ejecución similar a todos los efectos a un computador físico (excepto en el puro acceso físico al hardware simulado), con CPU (puede ser más de una), BIOS, tarjeta gráfica, memoria RAM, tarjeta de red, sistema de sonido, conexión USB, disco duro (pueden ser más de uno), etc.

[VMware](#) es similar a su homólogo Virtual PC, aunque existen diferencias entre ambos que afectan a la forma en la que el software interactúa con el sistema físico. El rendimiento del sistema virtual varía dependiendo de las características del sistema físico en el que se ejecute, y de los recursos virtuales (CPU, RAM, etc.) asignados al sistema virtual.

2.4. DIFERENCIA ENTRE DISCO ESTÁTICO Y DINÁMICO

El proceso de instalación de un hypervisor es muy sencillo, se instala un S.O. como

pueda ser Vmware, Xen Server, Hyper-V, habilitamos virtualización a nivel de kernel en cualquier Linux moderno y luego instalamos unas máquinas virtuales, como hacemos con virtual box, vmware workstation, pararells y demás hypervisores tipo 2.

Los pasos para realizar estas tareas no son nada complicados y en un corto tiempo podemos tener un entorno virtual funcionando correctamente, pero si nuestra meta es virtualizar sistemas complejos en producción, que necesiten alto rendimiento, puede que sea un poco más complicado; es muy importante diseñar un plan de virtualización para que, a futuro, no hayan inconvenientes.

Cuando se crea un disco duro virtual, no importa el sistema, podemos seleccionar si dicho disco tendrá un tamaño fijo o dinámico. Si es el segundo, en el disco físico se reserva el espacio utilizado aunque en el SO virtualizado veremos el total. Un ejemplo puede ser si creamos un disco de 100gb que Windows virtual verá como 100gb pero que realmente, en físico, ocupa 20gb. Esto es interesante para sobredimensionar, pero la escritura en disco será muy lenta. Un ejemplo podría ser lo que tarda en crearse un disco dinámico de 20 gb o de tamaño fijo. En el caso de tamaño fijo, el disco duro virtual se formateará con «ceros» todo el tamaño. Un poco de tiempo al principio nos dará mucho mas rendimiento más adelante.

Lo ideal es crear discos con controlador SCSI y no IDE para poder hacer ampliación de disco de forma más rápida. En modo IDE tendremos que añadir discos y ampliar volúmenes y esto complica las operaciones de administración del sistema. No hay diferencia en cuanto a rendimiento pero si mucha en cuanto a comodidad.

Las bases de datos son importantes; en el caso de usar SQL Server, se debe activar **PAGE LOCK MEMORY** en el Windows virtual, ¿la razón? SQL Server hace gestiones constantes en memoria para mantener registros consultados en cache y así agilizar las consultas, y por otra parte, tenemos un hypervisor con gestión de memoria dinámica, como Vmware, que intenta liberar RAM constantemente. Entonces es recomendable activar PAGE LOCK MEMORY mediante una GPO local en el Windows virtual y configurar la cuenta de servicio que arranca SQL para que mantenga en memoria bloqueada toda la ejecución y con esto prevenir la destrucción del cache.

Otra recomendación es si tenemos un sistema virtual con acceso intensivo a datos, separemos la ubicación física de los discos virtuales en distintos discos físicos. Recuerda que aunque sean virtuales, en algún momento la cabeza lectora del disco tendrá que alternar para leer/Escribir información de los distintos discos duros virtuales, por lo que separarlos aumenta el performance considerablemente.

En el caso de usar Hyper-V y tener instalado un Antivirus, cosa recomendable en cualquier sistema, es aconsejable excluir los ficheros de máquinas virtuales y los procesos VMMS.exe y VMWP.exe.

Otro truco importante para los sistemas virtualizados Windows es deshabilitar **PREFETCH**.

Los conocimientos requeridos para cada sistema, escenario y fabricante son diferentes como los son para los diferentes despliegues, pero no está de más tener en mente algunos trucos que se pueden aplicar de forma rápida y que van a ayudar a mejorar el rendimiento de nuestros sistemas virtuales.

BIBLIOGRAFIA

Comunicaciones y Redes de Computadoras. William Stallings.

WEBGRAFIA

<https://definicion.de/protocolo-de-red/#:~:text=Protocolo%20es%20el%20t%C3%A9rmino%20que,guiar%20una%20conducta%20o%20acci%C3%B3n.&text=Tambi%C3%A9n%20conocido%20como%20protocolo%20de,algo%20que%20constituye%20un%20est%C3%A1ndar>

<https://www.hostgator.mx/blog/que-es-una-direccion-ip/>

https://es.wikibooks.org/wiki/Tecnolog%C3%ADas_de_Internet/Enrutamiento#:~:text=En%20inform%C3%A1tica%20una%20ruta%20es,parte%20de%20ella%2C%20es%20determinada.&text=Cuando%20un%20paquete%20de%20IP,decidir%C3%A1%20qu%C

[3%A9%20hacer%20con%20%C3%A9l.](#)

<https://thehittoslab.blogspot.com/2016/10/las-clases-de-direcciones-ipv4-b-c-d-y-e.html>

<https://www.ionos.es/digitalguide/servidores/know-how/que-es-el-servidor-dns-y-como-funciona/>

<https://www.redeszone.net/tutoriales/internet/que-es-whois/>

<https://www.networkworld.es/telecomunicaciones/que-es-dhcp-y-como-funciona>

<https://www.tecnologia-informatica.es/uso-de-cmd-en-redes/>

<https://www.xatakamovil.com/conectividad/conoce-tu-router-i-direccion-ip-mascara-de-subred-y-puerta-de-enlace>

<https://www.netec.com/post/maquinas-virtuales-que-son-y-cuales-son-sus-tipos>

<https://www.catrian.com/virtualizacion-algo-sencillo-pero-que-no-siempre-se-hace-bien/>

Nro. Grupo 2

GLOSARIO

- **APPLETALK:** Este protocolo está incluido en el sistema operativo del computador Apple Macintosh desde su aparición y permite interconectar PC's y periféricos con gran sencillez para el usuario, ya que 110 requiere ningún tipo de configuración por su parte, el sistema operativo se encarga de todo.
- **DATAGRAMA:** Es un paquete de datos que constituye el mínimo bloque de información en una red de conmutación por datagramas, la cual es uno de los dos tipos de protocolo de comunicación por conmutación de paquetes usados para encaminar por rutas diversas dichas unidades de información entre nodos de una red, por lo que se dice que no está orientado a conexión. La alternativa a esta conmutación de paquetes es el circuito virtual, orientado a conexión.
- **ENRUTAR:** Una ruta es el camino que los datos deben realizar cuando viajan a través de una red desde un "host" a otro. El enrutamiento es el proceso por el cual la

ruta, o una parte de ella, es determinada. Una de las capacidades características de la Internet, en comparación con otras arquitecturas de red, es que cada router que recibe un paquete de datos determinará de inmediato por su cuenta cuál debe ser el próximo paso en la ruta. Cuando un paquete de IP es recibido por un router de la red, este decidirá qué hacer con él. Para realizar esta tarea consultará su tabla de enrutamiento.

- **ENMASCARAMIENTO IP** es una función de red que permite la conexión a otros miembros de la red a Internet a través de la conexión que ya posee la máquina que soporta el enmascaramiento. Esta técnica la utiliza el protocolo NAT que está incorporado en la mayor parte de routers. Así todos los ordenadores de la red pueden acceder a Internet a través de la conexión que tiene el router.

Nro. Grupo:2

- **MASCARA DE SUBRED:** Una máscara de subred es el principal modo en que TCP/IP limita el número de posibles direcciones con que tenga que tratar una máquina en un momento dado. La máscara de red es una manera de enmascarar o esconder unas partes de la red de otras. La máscara de red para su dirección determina cuántos de los números que componen la dirección IP serán vistos en realidad por otras máquinas como una dirección local de la red.

Por eso es importante que las computadoras en una misma parte local de la red usen la misma máscara de subred.

- **MULTIDIFUSIÓN:** o difusión múltiple (en inglés: multicast) es el envío de la información en múltiples redes a múltiples destinos simultáneamente. Antes del envío de la información, deben establecerse una serie de parámetros. Para poder recibirla, es necesario establecer lo que se denomina "grupo multicast". Este grupo multicast tiene asociada una dirección de Internet, de esta forma el emisor del mensaje multicast lo envía a uno o varios grupos y, posteriormente, el mensaje llega a los procesos que

están suscritos a dicho grupo, pudiendo estar un proceso suscrito a varios a la vez. La versión actual del protocolo de Internet (Internet Protocol o IP), conocida como IPv4, reserva las direcciones de tipo D para la multidifusión.

- **NAT:** La traducción de direcciones de red, también llamado enmascaramiento de IP o NAT (del inglés Network Address Translation), es un mecanismo utilizado por routers IP para intercambiar paquetes entre dos redes que asignan mutuamente direcciones incompatibles. Consiste en convertir, en tiempo real, las direcciones utilizadas en los paquetes transportados. También es necesario editar los paquetes para permitir la operación de protocolos que incluyen información de direcciones dentro de la conversación del protocolo. El tipo más simple de NAT proporciona una traducción una-a-una de las direcciones IP.

Nro. Grupo:2

- **NETBEUI.** Extended User Interface (Interfaz de usuario extendido para NetBIOS). Es la versión de Microsoft del NetBIOS (Network Basic Input Output System, sistema básico de entrada/salida de red), que es el sistema de enlazar el software y el hardware de red en los PCs. Este protocolo es la base de la red de Microsoft Windows para Trabajo en Grupo.
- **WHOIS** es un protocolo basado en petición y respuesta que se utiliza para efectuar consultas en una base de datos, la cual nos permite determinar el propietario de un nombre de dominio o una dirección IP en Internet.