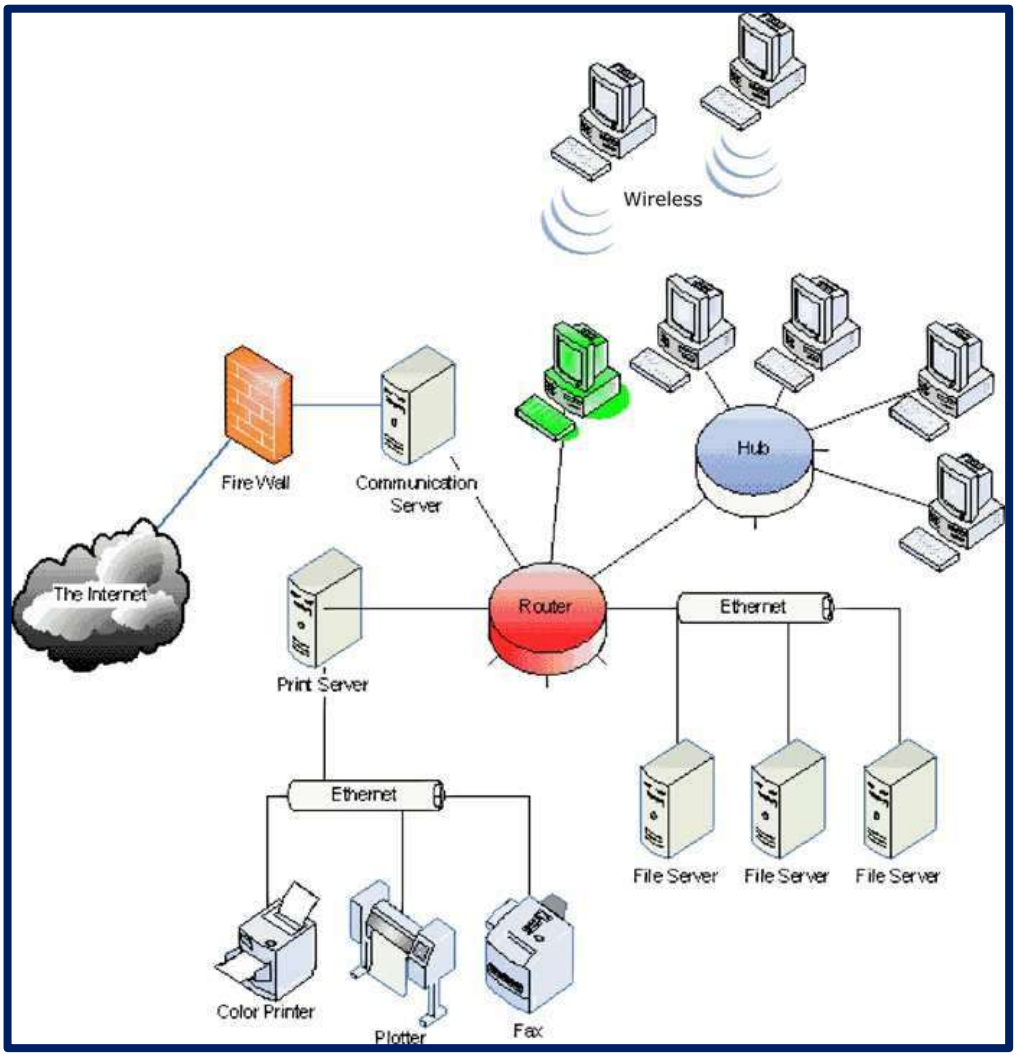
Conexión de Sistemas en Red



1. INTRODUCCIÓN. REDES DE ORDENADORES

Estudiados los elementos físicos de un sistema informático, vamos a iniciar en este tema el estudio de las redes de ordenadores.
Hoy día es cada vez menos probable encontrar ordenadores aislados. Cada vez más usuarios se conectan cada día a la red de redes para buscar información, comunicar sus opiniones al mundo o simplemente hablar un rato con los amigos.

1.1. CONCEPTOS BÁSICOS

Dos ordenadores conectados entre sí mediante algún medio, que se comunican y transmiten información forman una red. En la definición usamos dos palabras muy parecidas en significados pero que presentan diferencias a tener en cuenta: comunicación y transmisión.
Transmisión: es el transporte de la señal donde "viajan" los datos. Así la transmisión sólo se encarga de transportar sin importarle la información en sí. Para transportar la información se usan señales de diversos tipos: eléctricas, luminosas, acústicas, etc.
Comunicación: se refiere al transporte de la información. Cuando emisor y receptor se comunican no importa mucho la señal por la que lo hagan ni sus características físicas, sólo importan los datos que se están proporcionando ambos elementos en la red.
NOTA: Si existe comunicación existe transmisión, pero no siempre que se transmite se está comunicando.

2. VENTAJAS E INCONVENIENTES EN EL USO DE REDES

Entre las ventajas que proporciona el uso de redes de ordenador destacarnos:

- **Compartir información.** Evitamos tener duplicada la información; además el hecho de tener un fichero en varios lugares podría producir incoherencias en la información, ya que alguno de ellos podría estar más actualizado que otro.
- **Abaratamos costes.** Si tenemos una impresora compartida en una red podemos acceder a ella desde cualquier lugar de la misma en lugar de comprar una impresora para cada PC. Los recursos se comparten y ahorramos en gastos.
- **Repartimos el trabajo.** Una tarea puede dividirse en partes de forma que cada puesto en la red desempeñe una de esas tareas reduciendo la carga de trabajo.
- **Seguridad.** Las redes implementan mecanismos sofisticados de seguridad. Solo personas autorizadas pueden acceder a la red, pudendo restringir tanto la ejecución de aplicaciones como el acceso en un horario especifico.
- **Facilita la comunicación.** El uso de redes ha conseguido que personas alejadas en espacio que antes no podían comunicarse ahora sí lo hagan.

Son pocos los inconvenientes que vienen asociados a los sistemas en red, sin embargo, existen algunos relacionados sobre todo con la seguridad del mismo.

- **Ataques a la información.** Si los equipos de la red no son suficientemente seguros pueden ser atacados y vulnerada la información.
- **Mal uso o uso excesivo de la red.** Al igual que facilita las comunicaciones y relaciones sociales se debe tener especial cuidado en no hacer un uso excesivo de ellas, ya que puede perjudicar al individuo y provocar un aislamiento social.

3. CLASIFICACIÓN DE LAS REDES DE ORDENADORES

Las redes de ordenadores pueden clasificarse siguiendo diferentes criterios.

3.1. REDES SEGÚN LOS SERVICIOS QUE BRINDAN

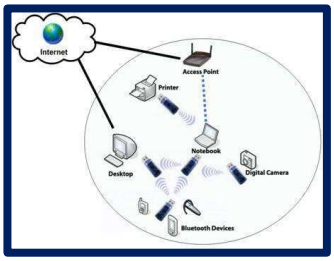
El objeto de una red fundamentalmente es el de compartir información y recursos. Según esto podemos distinguir: redes entre iguales (peer to peer) o redes cliente- servidor.

- **Redes cliente-servidor.** Son aquellas en las que algunos PC de la red tienen el rol de cliente de forma que demanda servicios y otros el de servidor, es decir, ofrece servicios. Normalmente, los equipos servidores suelen tener mejores prestaciones, aunque esto va en función del tipo de servicio que provea. Un servidor puede ser un ordenador en la red que comparte una simple carpeta. El rol de servidor o cliente va a depender de si comparte alguna información o recurso.
- **Redes entre iguales (peer to peer).** En una red entre iguales todos pueden ser clientes y servidores, ya que todos ofertan y demandan información y recursos.

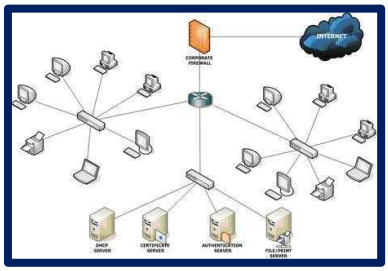
3.2. REDES SEGÚN EL ÁREA GEOGRÁFICA QUE OCUPAN

Según el área geográfica ocupada podemos distinguir los siguientes tipos de redes:

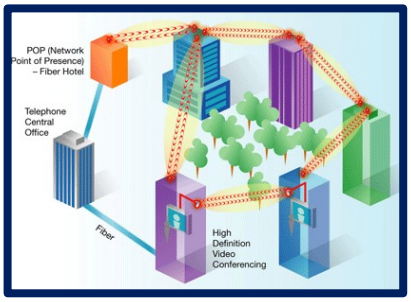
- **Redes de área personal (PAN, Personal Area Network)** Red formada por elementos que no pueden ubicarse a mucha distancia unos de otros para poder establecer comunicación Es el tipo de red que hoy día es habitual configurar en casa, una red formada por uno o varios PC de escritorio, algún PC portátil, móviles con bluetooth o infrarrojos, consola de videojuegos, etc.



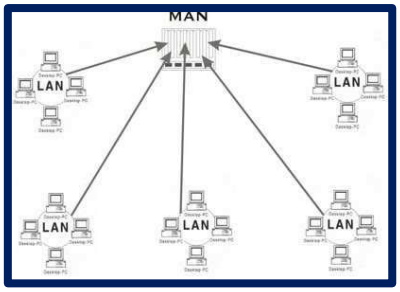
- **Red de área local (LAN, Local Area Network).** Red que ocupa una planta de un edificio o un edificio completo. Una LAN por lo general está administrada por una organización única.



- **Red de área de campus (CAN, Campus Area Network).** Red cuyos ordenadores están distribuidos por varios edificios dentro del mismo campus universitario o polígono industrializado, el espacio suele ser bastante mayor que el ocupado por una red LAN, varios edificios.



- **Red de área metropolitana (MAN, Metropolitan Area Network).** Red que ocupa municipios completos, ciudades o localidades completas. Una red MAN está compuesta por redes LAN que se interconectan usando determinados componentes de red.



- **Red de área extensa (WAN, wide area network).** Red que ocupa países y continentes.

4. ELEMENTOS DE UNA RED

Cuando hablamos de redes de ordenadores, teniendo en cuenta su definición de varios ordenadores conectados entre sí formando lo que se denomina circuito de datos, podemos deducir que en la red existen ordenadores que son emisores o receptores, medios por los que circula la información y dispositivos adicionales que permiten dicha comunicación.

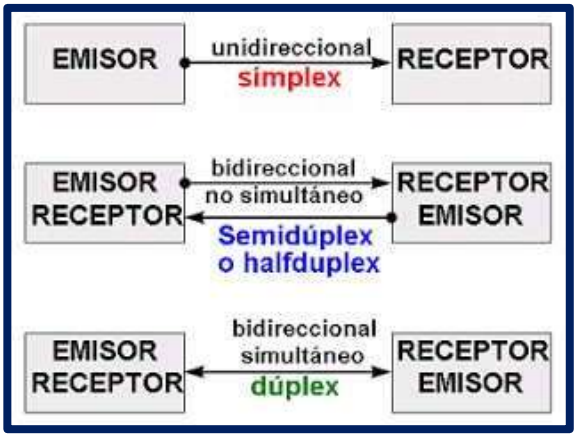
- **Ordenador, PC o Host**: elementos finales o iniciales de la transmisión de la información. En la red cualquier ordenador puede enviar un dato, ser emisor de información, o recibir un dato, ser receptor de la información. Existen determinados equipos que según la función que desempeñen puedan ser receptores o emisores. A estos dispositivos se les llama ETD (Equipo Terminal de Datos).
- **Medio:** elemento que se usa para la transmisión de la señal.
- **Transductor:** elementos ubicados junto a los ETD cuya misión es la de convertir la naturaleza de la señal para que pueda ser transmitida por el medio físico. Se denomina ECD (Equipo de Comunicación de Datos).
- **Otros elementos del sistema de comunicación:** dispositivos de red que se encargan de ampliar la señal que viaja por un medio concreto, repetir la misma, etc.

5. EXPLOTACIÓN DEL CIRCUITO DE DATOS

5.1. TIPOS DE COMUNICACIONES

Teniendo en cuenta el modo por el que circulan los datos, podemos distinguir tres formas en las que se produce la comunicación entre dos ETD (Equipo Terminal de Datos): Simplex, Half-duplex y Duplex.

- **Comunicación simplex.** En este tipo de comunicación existe un solo emisor y un solo receptor, no pudiendo en ningún momento intercambiar sus papeles. Cuando comienza la comunicación el emisor empieza a emitir estando el receptor siempre en espera.
- **Comunicación half-duplex o semiduplex.** En este tipo de comunicación un extremo y otro de la misma puede ser emisor y receptor, pero nunca al mismo tiempo. Cuando uno de los dos extremos emite, el otro espera a recibir la información. Cuando la información llega al receptor este puede optar por convertirse en emisor o no. Así tenemos comunicación bidireccional pero no simultánea.
- **Comunicación dúplex.** En este tipo de comunicación un extremo y otro actúan como emisor y receptor, y pueden transmitir la información al mismo tiempo. Hablamos de una comunicación bidireccional y simultánea. Ejemplo claro de este tipo de comunicación es la comunicación telefónica. En el momento que se establece comunicación entre los dos abonados ambos pueden hablar a la vez sin esperar turno de palabra.



5.2. TIPOS DE TRANSMISIONES

Cuando hablamos de la transmisión en sí, es decir, del transporte de la señal, podemos distinguir varios tipos: **Síncrona y asíncrona** o **Serie y paralela**.

El sincronismo es el procedimiento por el que emisor y receptor se ponen de acuerdo sobre el momento concreto en el que va a comenzar y acabar la transmisión. Si se produce un error de sincronismo, la señal se desplazará del emisor al receptor, pero al no saber dónde empieza la información o dónde acaba, no podrá ser interpretada correctamente.

Cuando hablamos de **transmisión asíncrona**, el proceso de sincronización se hace palabra a palabra de forma que se indica cuándo empezamos a transmitir y cuándo acabamos en cada palabra mediante el uso de bits delimitadores, Por ejemplo, si el canal está en silencio (transmitiendo cero lógicos), se puede indicar que se va a comenzar a transmitir emitiendo un 1 al receptor. De igual modo, cuando acabe la transmisión se pueden agregar varios bits de stop.

En una **transmisión síncrona**, la transmisión se realiza de forma constante bit a bit existiendo determinados bits de control.

En una **transmisión serie** la información circula por una única línea de datos de forma secuencial, es decir, los bits van uno a uno detrás de otro, por el mismo canal. En la **transmisión paralela** la información circula por varias líneas de comunicación, es decir, se transmiten simultáneamente varios bits a la vez.

NOTA: Puede parecer que la transmisión paralela es la mejor de las opciones; sin embargo, debemos pensar un poco antes de afirmarlo, ya que al existir mayor número de líneas también aumentan las interferencias entre ellas.

6. ARQUITECTURA DE UNA RED

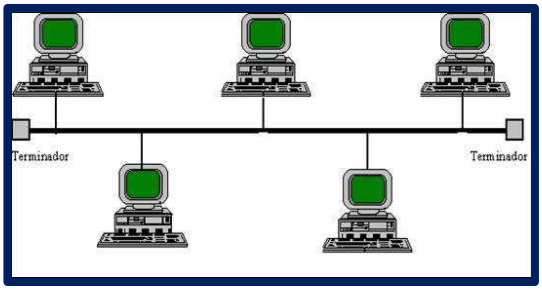
Una arquitectura de red define la forma en la que se conectan los nodos o host de red, qué proceso deben seguir cuando quieran comunicarse con otro host, teniendo en cuenta el medio del que disponen. Así, cuando hablamos de arquitectura de red estamos hablando de: **topología de la red, método de acceso al medio y protocolo o familias de protocolos de comunicación.**

6.1. TOPOLOGÍA

La topología de una red refiere la forma física de la misma. Normalmente, hablamos de topología cuando trabajamos con redes cableadas, de forma que el dibujo que forman los PC con los cables o medios físicos que los unen constituyen ésta. En redes inalámbricas también se distinguen topologías, por ejemplo, topología **ad-hoc** en las que existe una comunicación punto a punto entre dos elementos de red.
En este apartado estudiaremos las topologías de redes cableadas.

→ TOPOLOGÍA EN BUS

Todos los ordenadores están conectados a un mismo medio físico (único cable principal). Esta topología era implementada mediante cable coaxial, siguiendo el estándar IEEE 802.3. El medio usado tiene múltiples accesos para que los PC puedan conectarse a él y en los extremos, para evitar la producción de ECO o reflexiones (la señal transmitida rebota en un extremo y vuelve al medio), se colocaban unos terminadores que absorbían la señal.
Una de las **desventajas de este tipo de redes era la rotura del medio físico usado, dejando inservible toda la red**.



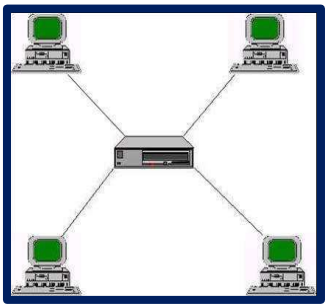
→ TOPOLOGÍA EN ESTRELLA

En esta topología la red forma una estrella, existiendo un nodo o elemento que centraliza todo el paso de información. Cada estación de trabajo se conecta punto a punto con el nodo central, de forma que si quieren transmitir información envían ésta al nodo central y éste se encargará de retransmitir a todos o al PC destino según el tipo de dispositivo central que tengamos.
Ventajas:

- Son redes más seguras ya que toda la información pasa por el nodo central, pudiendo detectarse posibles fallos en la comunicación.
- Si un segmento de la red deja de funcionar no repercute en el resto (cuando hablamos de segmento nos referimos a la conexión entre una estación de trabajo y el nodo central)

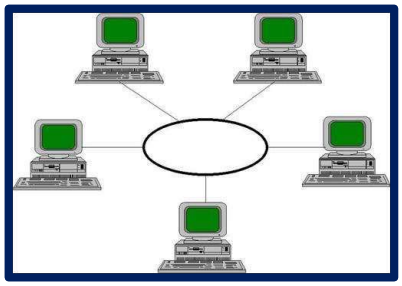
Inconvenientes:

- El inconveniente principal de este tipo de redes es el denominado cuello de botella. Si toda la información debe pasar por el nodo central, a pequeñas cantidades de información no pasa nada pero cuando el volumen a transferir aumenta, es posible que el nodo central se convierta en un cuello de botella de modo que la red se vea ralentizada.
- Mal funcionamiento del nodo central o caída del mismo. Si el nodo central deja de funcionar, la red cae ya que es el elemento principal de la misma.
- Hay que usar gran cantidad de cable.



→ TOPOLOGÍA EN ANILLO

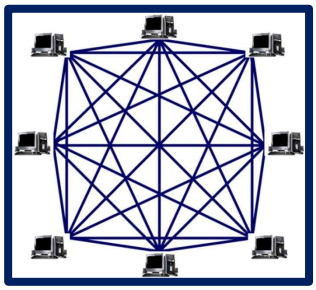
Los ordenadores que tienen esta topología forman un anillo, de manera que observamos una red en la que de dos en dos se conectan punto a punto los host, cerrando el circuito el primer y último PC.



→ TOPOLOGÍA EN MALLA

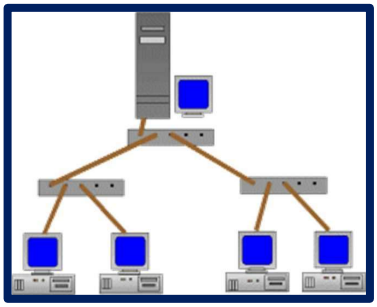
Este tipo de topología dibuja una red en la que todos los elementos están conectados punto a punto con uno o más de los componentes de la red. Si cada host se conecta con todos los demás host tenemos una malla completa o una topología de interconexión total, en la que cada PC debe tener varias interfaces de red.

Este tipo de topología tiene la ventaja de que si un host deja de funcionar los demás continúan con su actividad normal; todos pueden seguir comunicándose con todos a excepción del elemento que dejó de funcionar.



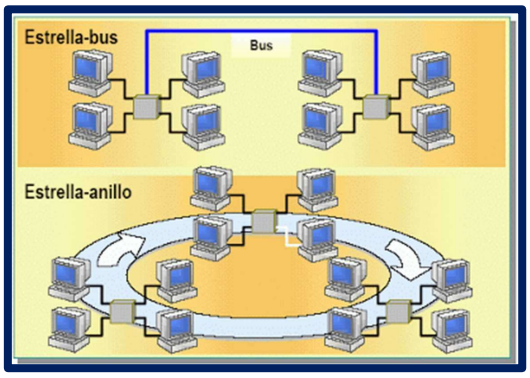
→ TOPOLOGÍA EN ÁRBOL

Esta topología es una extensión de la topología en bus, donde varias líneas de buses se conectan a un bus central que propaga la señal a éstos. Tenemos diferentes niveles a los que se conectan los hosts formando un árbol. En estas topologías tenemos la ventaja de que si un bus secundario deja de funcionar, el resto de buses continúan con la transmisión de información; aunque si cae el bus principal la red queda inservible.



→ TOPOLOGÍAS MIXTAS

Hablamos de topologías mixtas en redes que comparten al menos dos de las topologías estudiadas en este apartado, por ejemplo, la red de una empresa que en una zona tiene una topología en bus y en otra su distribución es en estrella.



6.2. MÉTODO DE ACCESO AL MEDIO

El **método de acceso** al medio dicta las reglas que deben seguir los hosts de una red a la hora de usar el medio para transmitir información. En función del tipo de red que usemos el acceso al medio será diferente.
Cuando hablamos de método de acceso al medio pensamos que existen varios ordenadores conectados al mismo medio y todos quieren transmitir en un momento dado. A la hora de hacerlo deben asegurarse de que este esté libre. Asegurarse de la falta de ocupación del medio requiere de métodos concretos que eviten colisiones (dos PC que envíen información a la vez) entre otros problemas.

6.3. PROTOCOLO O FAMILIA DE PROTOCOLOS

Conjunto de reglas bien definidas y acordadas por las dos partes que establecen la comunicación y regulan algún aspecto de esta. Normalmente, los protocolos suelen ser estándares desarrollados por ciertas organizaciones o los propios fabricantes y tienen rigor legal.
Los protocolos son de suma importancia en una red ya que dictan las normas a seguir para que se produzca la comunicación entre emisor y receptor.
Algunas de las organizaciones dedicadas a la estandarización son:

- ANSI (American National Standards Institute). Dedicada a la estandarización orientada a redes LAN y WAN.
- IEEE (Institute of Electrical and Electronics Engineers. Dedicada como la anterior a la estandarización en redes LAN y WAN.
- ISO (International Organization for Standardization). Desarrolla entre otras cosas el modelo de referencia OSI 3.
- TI4 (Telecommunications Industry Association).
- W3C (World Wide Web Consortium).

6.4. CAPAS O NIVELES

La arquitectura de red es algo muy complejo que debe contemplar muchos aspectos. Por eso, cuando se diseña una arquitectura ésta se divide en capas o niveles de forma que se reparten las funciones. El concepto de "divide y vencerás" tan usado en programación estructurada. Una arquitectura muy compleja se divide en capas, encargándose cada una de ellas de una parte del proceso de comunicación. Las capas adyacentes se transmiten información gracias a una interfaz (conjunto de funciones por las que la capa de más arriba pide servicios a la que está justamente debajo).

6.5. MODELO DE REFERENCIA OSI

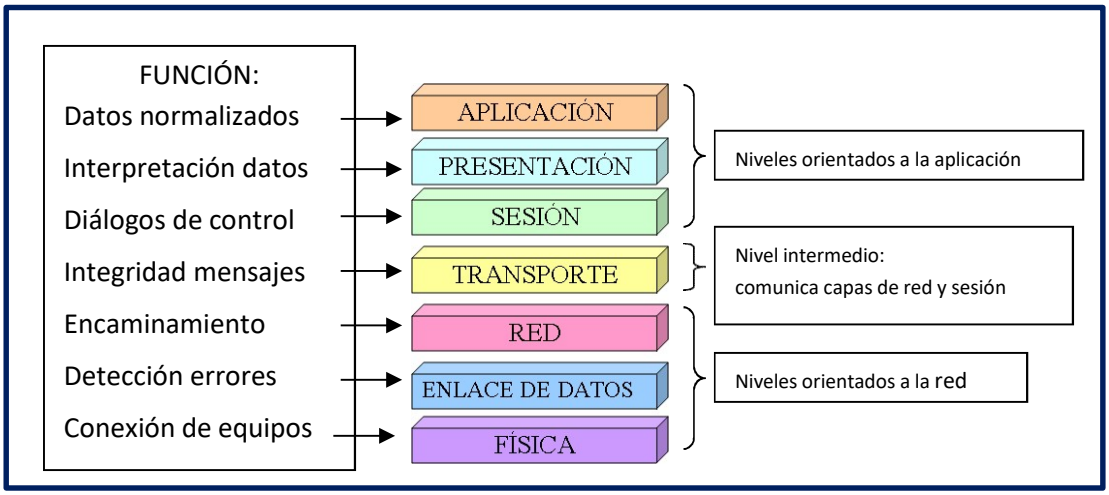
OSI (Open Systems Interconnection, Interconexión de Sistemas Abiertos) es el modelo de referencia creado por la ISO que adaptan muchos fabricantes para el desarrollo de una arquitectura de red constituida por capas. No es una arquitectura sino un modelo a seguir a partir del que podemos desarrollar protocolos para la conexión de diferentes tipos de redes. Es un modelo teórico.
El modelo OSI propone un modelo compuesto por siete capas o niveles, de modo que la primera de ellas es la más cercana al nivel físico y el número siete la más cercana al usuario.

6.5.1. Niveles del modelo de referencia OSI

Las capas o niveles del modelo se denominan: **Aplicación, Presentación, Sesión, Transporte, Red, Enlace** y **Físico**.
Los niveles se dividen en:

- **Niveles orientados a la red**
- **Niveles orientados a la aplicación**.

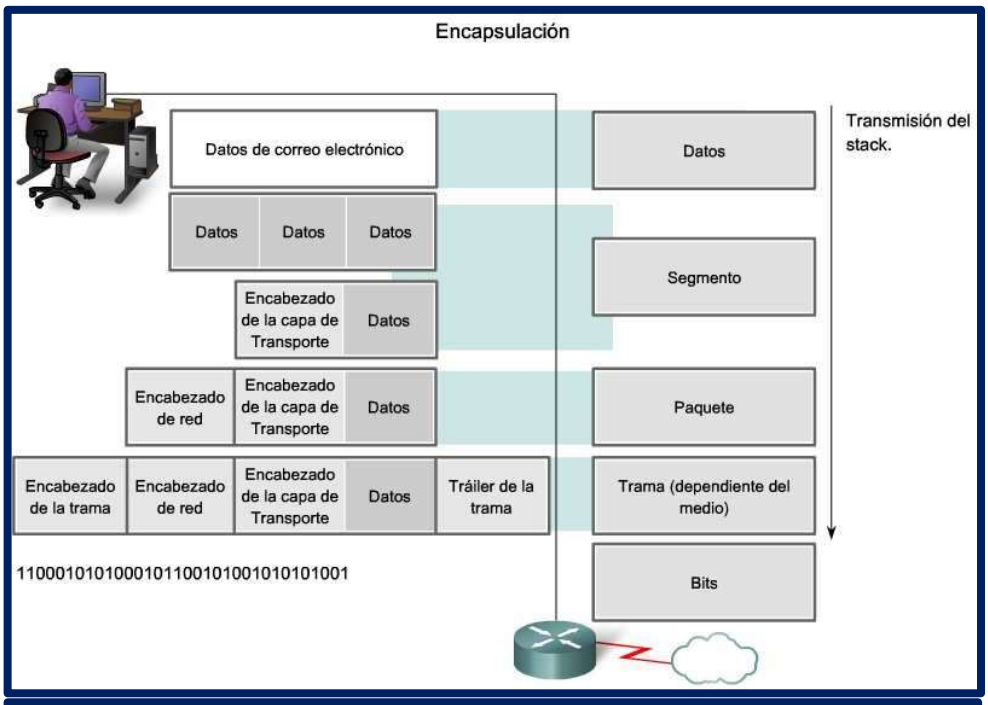
El primer grupo de niveles lo forman las capas de red, enlace y física; mientras que los orientados a la aplicación son sesión, presentación y aplicación.
La capa de transporte no se incluye en ninguno de estos grupos ya que se considera un nivel intermedio cuya función es principalmente la de comunicar la capa de red con la de sesión.

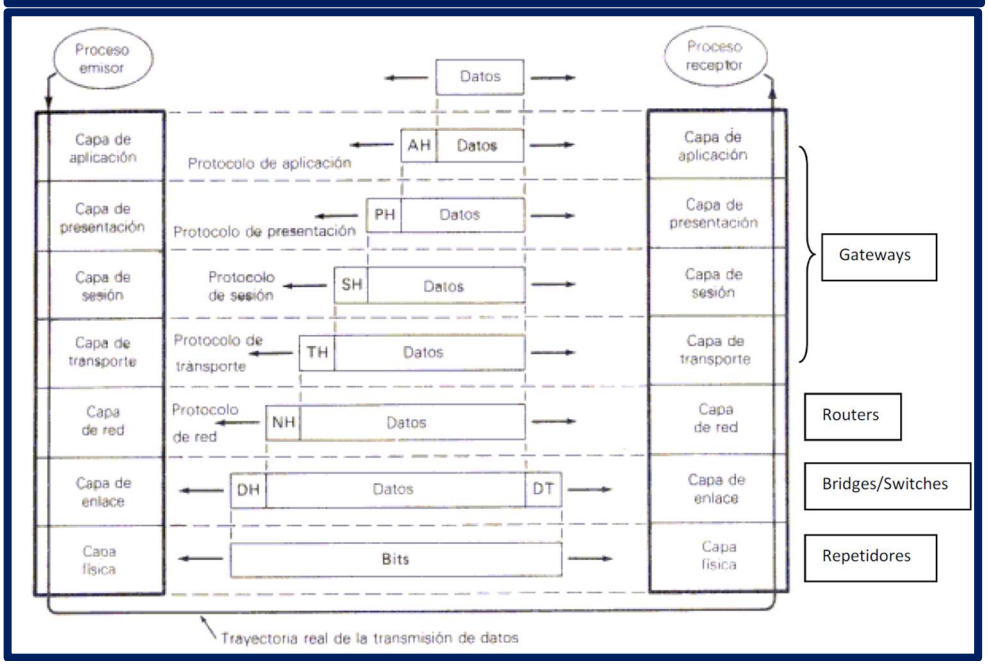


- **Aplicación:** Es la capa más cercana al usuario y es en la que se definen los protocolos que utilizan las aplicaciones y procesos de usuario. Se definirán aquí protocolos como el HTTP, SMTP, POP, etc.
- **Presentación:** Es la capa encargada de presentación de la información. Imaginemos que queremos comunicar dos PC, uno usa codificación EBCDIC y otra codificación ASCII. Si no existiera esta capa la comunicación o entendimiento entre los dos PCs no serían posibles, ya que "hablan lenguajes distintos". Así esta capa se ocupará de la sintaxis y la semántica de la información que se quiere transmitir. Determina el formato de las comunicaciones, así como adaptar la información al protocolo que se esté usando.
- **Sesión:** Esta capa se encarga de iniciar una sesión para cada comunicación que se quiera establecer. Así, cada vez que algún host quiere convertirse en emisor se crea y mantiene una sesión de forma que se pasa la información a la capa de transporte para que pueda comenzar a ser tratada y posteriormente enviada a través del medio físico elegido. Mantiene y controla el enlace entre los dos extremos de la comunicación.
- **Transporte:** Este nivel es básicamente un intermediario entre las capas de sesión y red. Su labor principal es la de trocear la información procedente de la capa de sesión para que sea aceptada por la de red. Se encarga de que los paquetes de datos tengan una secuencia adecuada y de controlar los errores.
  La capa de transporte utiliza un esquema de direccionamiento llamado número de puerto. Los números de puerto identifican las aplicaciones y los servicios de la capa de aplicación que son el origen y el destino de los datos. Los programas del servidor generalmente utilizan números de puerto predefinidos comúnmente conocidos por los clientes. Mientras examinamos los diferentes servicios y protocolos de la capa de aplicación de TCP/IP, nos referiremos a los números de puerto TCP y UDP normalmente asociados con estos servicios. Algunos de estos servicios son:
  - → Sistema de nombres de dominios (DNS) - TCP/UDP puerto 53
  - → Protocolo de transferencia de hipertexto (HTTP) - TCP puerto 80
  - → Protocolo simple de transferencia de correo (SMTP) - TCP puerto 25
  - → Protocolo de oficina de correos (POP) - TCP puerto 110
  - → Telnet - TCP puerto 23
  - → Protocolo de configuración dinámica de host - UDP puertos 67 y 68
  - → Protocolo de transferencia de archivos (FTP) - TCP puertos 20 y 21

Capas Modelo OSI	Protocolos
APLICACIÓN	TELNET, FTP, SNMP, NNTP, SSH, SMTP, POP3, DNS, RTP, NFS, HTTP
PRESENTACIÓN	ASN.1
SESIÓN	NetBIOS
TRANSPORTE	TCP, UDP
RED	ARP, IP(IPv4/IPv6), ICMP, X.25
ENLACE DE DATOS	ETHERNET, FAST ETHERNET, GIGABIT ETHERNET, FDDI, ATM, HDLC
FISICA	CGI, MIME, IEEE

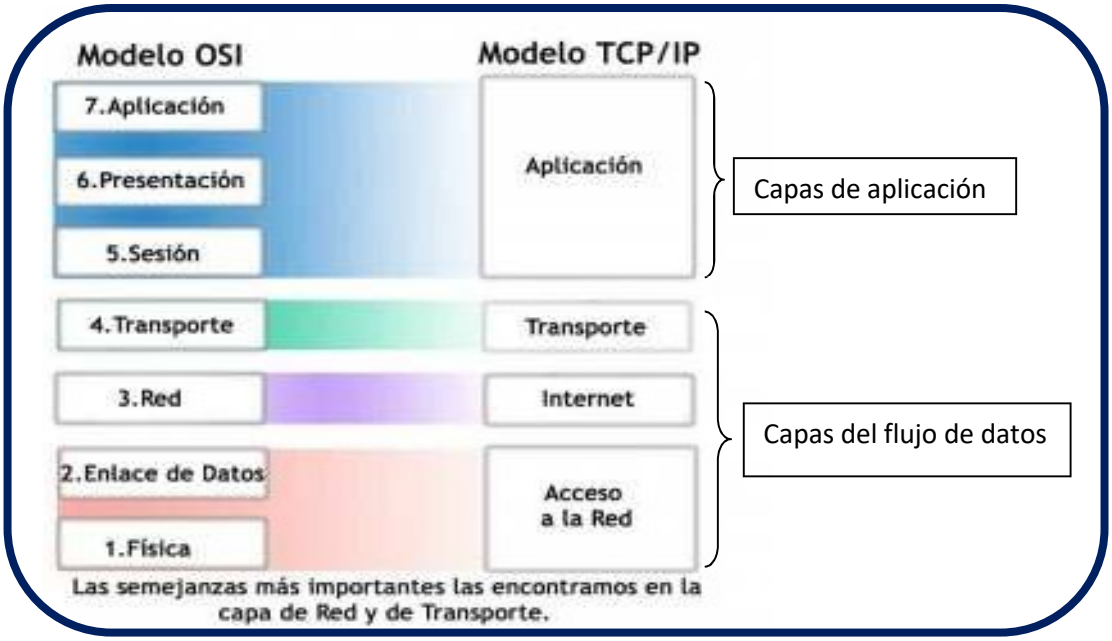
- **Red:** Se encarga de buscar rutas óptimas por las que puede viajar la información troceada previamente en el nivel anterior (Transporte). Separa los datos en paquetes, determina la ruta que tomarán los datos y define el direccionamiento.
- **Enlace de datos:** La capa de enlace de datos debe asegurarse de que la información a enviar esté libre de errores. La información troceada anteriormente se divide tratándose como bloques de datos denominados tramas. En esta capa, se detectan errores solicitándose posibles reenvíos de tramas, tramas duplicadas, se solventan problemas de flujo, diferencias de velocidades de trasmisión, etc. Empaqueta los datos para transmitirlos a través de la capa física. En esta capa se define el direccionamiento físico utilizando las conocidas direcciones MAC. Además, se encarga del acceso al medio, el control de enlace lógico o LLC y de la detección de errores de transmisión, entre otras cosas.
- **Física:** Capa en la que se definen los aspectos relacionados con la transmisión física de la red, datos de la señal, voltajes, tipos de cables, conectores, etc. Se encarga de las conexiones físicas, incluyendo el cableado y los componentes necesarios para transmitir la señal.



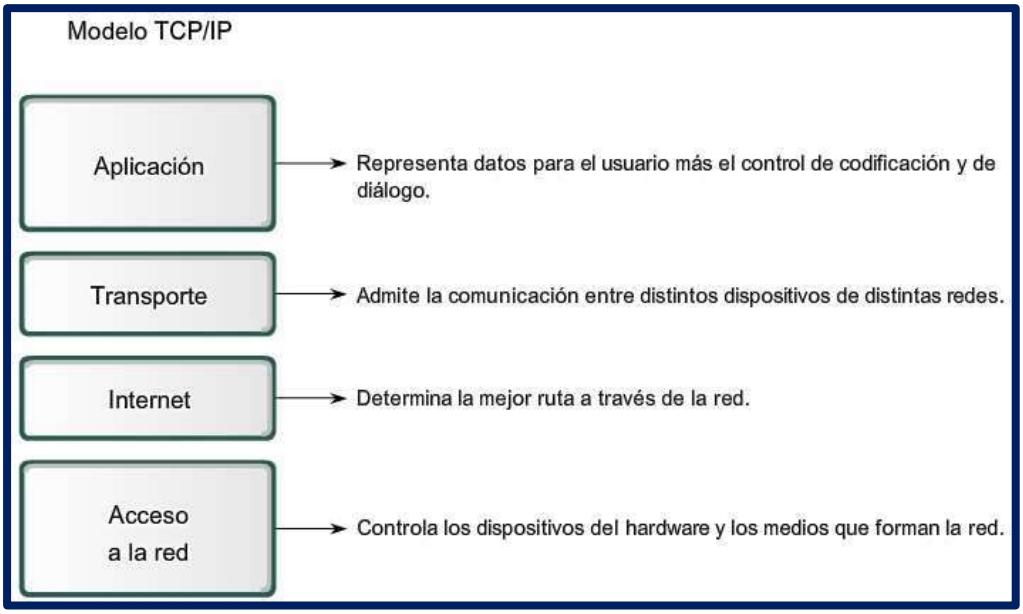


6.6. ARQUITECTURA TCP/IP

A veces confundimos esta arquitectura de red con un protocolo, pero es una arquitectura compleja y la más usada, ya que es la base de las comunicaciones en Internet.
Es el primer modelo de protocolo en capas para comunicaciones en redes y se conoce con el nombre de **modelo de Internet** o **modelo TCP/IP** (Transmission Control Protocol/Internet Protocol).
TCP/IP es una **arquitectura formada por gran variedad de protocolos**, siendo los más importantes los TCP/IP de los que adopta su nombre.



El **modelo de capas TCP/IP** **prescinde de las capas de Presentación y Sesión** debido a que la mayoría de las aplicaciones no las usan.
En la **capa de aplicación** encontramos todos los **protocolos de alto nivel** como http, smtp, pop, etc.
Además, **unifica las capas de enlace y física** en una única red llamada **red**, **subred** o **host a red**. La capa de red no está demasiado definida en la arquitectura TCP/IP, contempla redes, 802.3, 802.5, etc.
La mayoría de los modelos de protocolos describen una pila de protocolos específicos del proveedor. Sin embargo, puesto que el modelo TCP/IP es un estándar abierto, una compañía no controla la definición del modelo. Las definiciones del estándar y los protocolos TCP/IP se explican en un foro público y se definen en un conjunto de documentos disponibles al público. Estos documentos se denominan Solicitudes de comentarios (RFC: Request for comments). Contienen las especificaciones formales de los protocolos de comunicación de datos y los recursos que describen el uso de los protocolos.

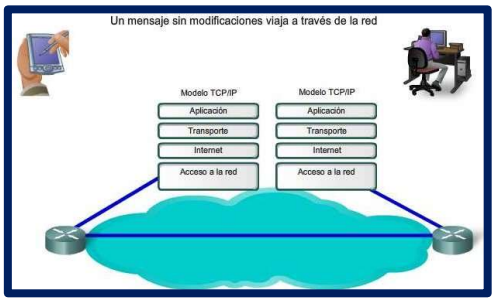


El **modelo TCP/IP describe la funcionalidad de los protocolos** que forman la suite de protocolos TCP/IP. Estos protocolos, que se implementan en los hosts emisores y receptores, interactúan para brindar una entrega extremo a extremo de las aplicaciones a través de la red.

Un proceso de comunicación completo incluye estos pasos:

1. Creación de datos en la capa de aplicación del dispositivo final de origen.
2. Segmentación y encapsulación de datos a medida que pasan por la pila de protocolos en el dispositivo final de origen.
3. Generación de datos en los medios en la capa de acceso a la red.
4. Transporte de los datos a través de la red, la cual está compuesta por medios y por cualquier dispositivo intermedio.
5. Recepción de los datos en la capa de acceso a la red del dispositivo final de destino.
6. Desencapsulación y reensamblaje de los datos a medida que pasan por la pila en el dispositivo de destino.
7. Transmisión de estos datos a la aplicación de destino en la capa de aplicación del dispositivo final de destino.

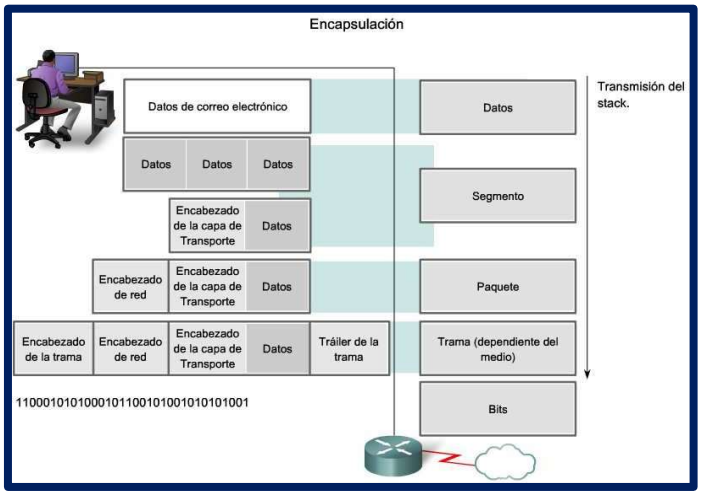
La encapsulación es el proceso por el cual se envuelven datos en un encabezado de protocolo en particular.



Unidad de datos del protocolo y encapsulación

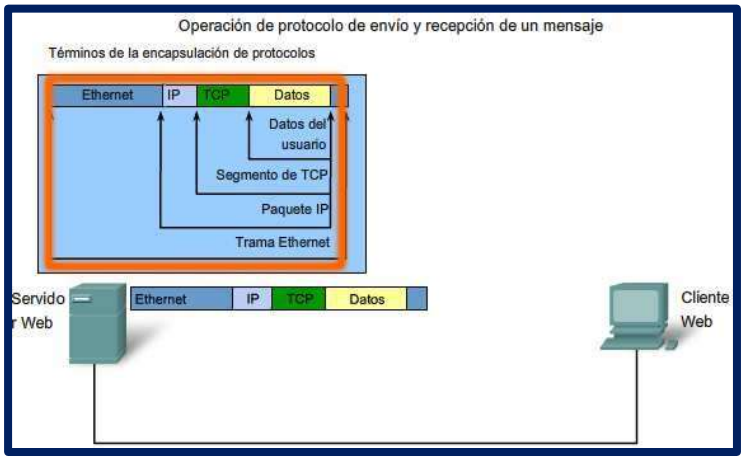
Mientras los datos de la aplicación recorren las capas del modelo varios protocolos les agregan información en cada nivel. Esto comúnmente se conoce como **proceso de encapsulación**.
La forma que adopta una sección de datos en cualquier capa se denomina **Unidad de datos del protocolo (PDU)**. Durante la encapsulación, cada capa encapsula las PDU que recibe de la capa inferior de acuerdo con el protocolo que se utiliza. En cada etapa del proceso, una PDU tiene un nombre distinto para reflejar su nuevo aspecto. Aunque no existe una convención universal de nombres para las PDU, las denominaremos de acuerdo con los protocolos de la suite de TCP/IP:

- **Datos:** término general que se utiliza en la capa de aplicación para la PDU
- **Segmento:** PDU de la capa de transporte
- **Paquete:** PDU de la capa de internet
- **Trama:** PDU de la capa de acceso a la red
- **Bits:** PDU que se utiliza cuando se transmiten datos físicamente por el medio

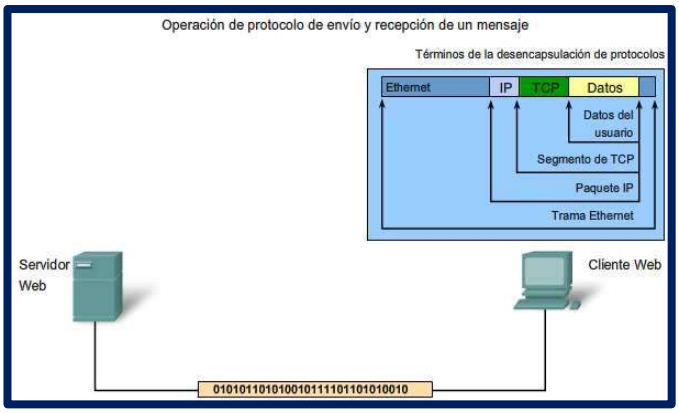


Proceso de envío y recepción

Cuando se envían mensajes en una red, la pila de protocolos de un host opera desde las capas superiores hacia las capas inferiores. En el ejemplo del servidor Web podemos utilizar el modelo TCP/IP para ilustrar el proceso de envío de una página Web HTML a un cliente.
El protocolo de la capa aplicación, HTTP, comienza el proceso entregando los datos de la página Web con formato HTML a la capa de transporte. Allí, los datos de aplicación se dividen en segmentos de TCP. A cada segmento de TCP se le otorga una etiqueta, denominada encabezado, que contiene información sobre qué procesos que se ejecutan en el ordenador de destino deben recibir el mensaje. También contiene la información para habilitar el proceso de destino para reensamblar los datos de nuevo en su formato original.
La capa de transporte encapsula los datos HTML de la página Web dentro del segmento y los envía a la capa de Internet, donde se implementa el protocolo IP. Aquí, el segmento de TCP se encapsula en su totalidad dentro de un paquete IP que agrega otro rótulo denominado encabezado IP. El encabezado IP contiene las direcciones IP de host de origen y de destino, como también la información necesaria para entregar el paquete a su proceso de destino correspondiente.
Luego el paquete IP se envía al protocolo Ethernet de la capa de acceso a la red, donde se encapsula en un encabezado de trama y en un tráiler. Cada encabezado de trama contiene una dirección física de origen y de destino. La dirección física identifica de forma exclusiva los dispositivos en la red local. El tráiler contiene información de verificación de errores. Finalmente, los bits se codifican en el medio Ethernet mediante la NIC del servidor.



Trama: información de control que se agrega a los datos cuando éstos se encapsulan para la transmisión por la red.
Este proceso se invierte en el host receptor. Los datos se desencapsulan mientras suben la pila hacia la aplicación del usuario final.



7. ELEMENTOS DEL NIVEL FÍSICO

La capa o nivel físico es la que establece tipos de medios a usar para la transmisión, características físicas del medio, niveles de voltaje para representar ceros y unos, etc.
El medio físico utilizado es de gran importancia, ya que las características del mismo pueden perjudicar o no a la señal, permitiendo por ej. el exceso de ruido5 o una mayor velocidad. Se pueden transportar señales eléctricas, electromagnéticas, luminosas, etc., con lo que el medio físico se debe adecuar a las mismas. Los medios físicos se clasifican en dos tipos: medios físicos guiados y medios físicos no guiados.

MEDIOS FÍSICOS GUIADOS

Son aquellos en los que la señal se transmite de forma que el medio guía esta. Existe un elemento, como cable de cobre, fibra de vidrio, etc., que se encarga de establecer un camino por el que debe circular la portadora. Entre los medios físicos guiados estudiaremos: cable par trenzado, cable coaxial y fibra de vidrio.

MEDIOS FÍSICOS NO GUIADOS

La información se envía mediante señales electromagnéticas que se propagan en el medio libre, con o sin atmósfera. Para que se produzca la transmisión de información deben existir antenas que se encarguen de la emisión y recepción de estas ondas.
Las transmisiones no guiadas pueden ser: direccional y omnidireccional.
Transmisión direccional: Es aquella en la que la señal se concentra para ser enviada en una única dirección, de forma que no deben existir obstáculos entre antena emisora y receptora que obstaculicen la transmisión.
Transmisión omnidireccional. La información se envía en todas direcciones con lo que puede ser recibida por varias antenas.

DISPOSITIVOS DE RED

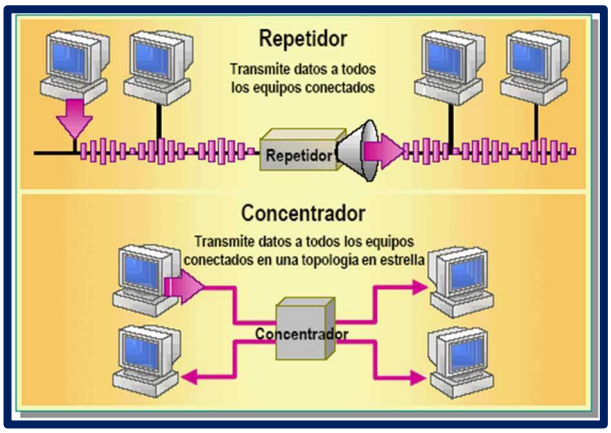
En el Apartado 6.5 estudiábamos el modelo de referencia OSI, dividido en siete capas. Cada una de esas capas con una función bien determinada. Las redes que hoy conocemos siguen como referencia este modelo, de forma que deben existir dispositivos o componentes software que se adapten a la funcionalidad de cada una de ellas. Así, a la hora de instalar una red debemos tener en cuenta que existen dispositivos que trabajan a nivel físico, a nivel de enlace y a nivel de red, desempeñando las funciones que estas capas deben realizar en la teoría.

1. Dispositivos hardware de nivel físico

MODEM
Dispositivo encargado de modular/demodular la señal. Cuando la información tiene que ser enviada ha de serlo a través de un medio físico concreto con determinadas características, así, la señal debe ser adaptada al medio físico (debe ser modulada). Cuando la señal se recibe debe realizarse el proceso inverso (debe ser demodulada). Existen dos tipos: interno y externo.
Hoy día, cuando se habla de este dispositivo nos referimos normalmente a aquel que se encarga de conectar nuestra red de casa a la red de área extensa. Son ejemplo de estos adaptadores: modem RDSI (conectan nuestra red interna a la red digital RDSI), modem ADSL (conexión a través de la línea telefónica), modem cable (conexión a través de líneas coaxiales implementadas en un principio para ver televisión) y modem inalámbrico (conexión mediante antena a una red pública).

REPETIDORES

Se encargan de amplificar la señal digital, debido a que en largas distancias ésta se atenúa pudiendo llegar a desvanecerse. Estos dispositivos restauran la señal original permitiendo que alcance el equipo receptor de la información.



CONCENTRADORES DE CABLEADO

También denominados repetidores multipuerto o Hub Ethernet. Es un dispositivo cuya misión es la de repetir la información que recibe por todas sus salidas o puertos, y conectar todos los nodos de la red. Existen dos tipos: repetidores pasivos que básicamente se encargan de conectar todos los nodos de la red permitiendo su comunicación y los repetidores activos que además de repetir y comunicar la señal, la amplifican y regeneran antes de ser reenviada.

2. Dispositivos hardware de nivel de enlace

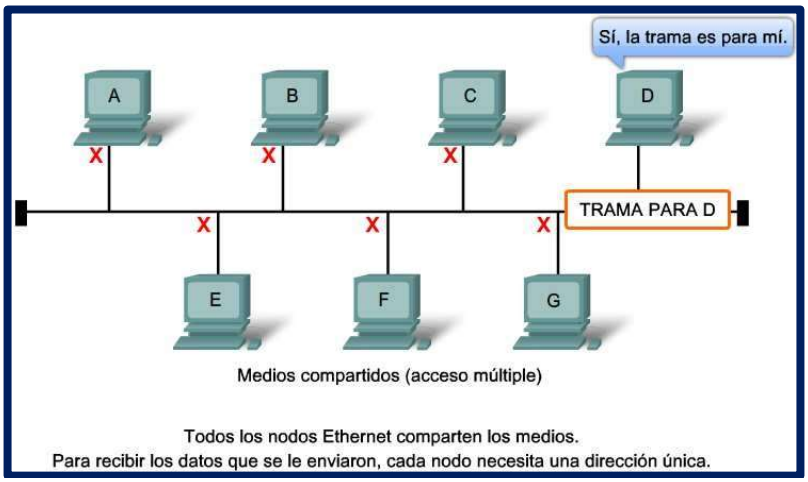
El uso de dispositivos de nivel físico para conectar los nodos de una red es una solución sencilla y útil cuando el número de ordenadores de la red es escaso y no esperamos un rendimiento elevado de la misma. En el momento en el que comenzamos a agregar nuevos nodos, la red se ralentiza y no es capaz de gestionar redes relativamente grandes.

Al usar un repetidor (hub) para conectar una red, cada vez que un nodo quiere enviar una información esta se propagará por todos los puertos del dispositivo, de forma que el dato llega a todas las estaciones, todas rechazan el paquete a excepción del receptor que lo interpreta. De este modo, si la tasa de transferencia de la red es de 10 Mbps, al usar todos los canales para retransmitir la información, en un repetidor de 10 puertos esta tasa se verá dividida entre 10, de forma que la tasa de transferencia se reducirá a 1 Mbps para cada puerto. Si el número de puertos aumenta, disminuirá la velocidad a la que transmiten cada uno de ellos y hará que la red deje de rendir.

Además, puede ocurrir que tengamos una única LAN montada en un edificio o varias, y en el caso de que sean varias redes, estas pueden seguir diferentes estándares, 802.3, 802.11, 802.5, etc., y deben estar conectadas entre sí. Esta casuística solo es capaz de resolverla un dispositivo de nivel de enlace.

Los dispositivos de nivel de enlace trabajan con direcciones MAC (Media Access Control / CONTROL DE ACCESO AL MEDIO) o direcciones físicas. Una dirección MAC está compuesta por 48 bits, 6 bloques de números hexadecimales, e identifican de forma única a una tarjeta o dispositivo de red.

Este identificador único, denominado dirección de Control de acceso al medio (MAC), se creó para ayudar a determinar las direcciones de origen y de destino dentro de una red de área local.



Recordad que la dirección MAC se agrega como parte de una PDU de Capa 2. Una dirección MAC es un valor binario de 48 bits expresado como 12 dígitos hexadecimales.

El valor de la dirección MAC es el resultado directo de las normas implementadas por el IEEE para proveedores con el objetivo de garantizar direcciones únicas para cada dispositivo Ethernet.

Todas las direcciones MAC asignadas a una NIC u otro dispositivo Ethernet deben utilizar el OUI que se le asignó a dicho proveedor como los 3 primeros bytes.

La dirección MAC se graba en la ROM (memoria de sólo lectura) de la NIC. Esto significa que la dirección se codifica en el chip de la ROM de manera permanente (el software no puede cambiarla).

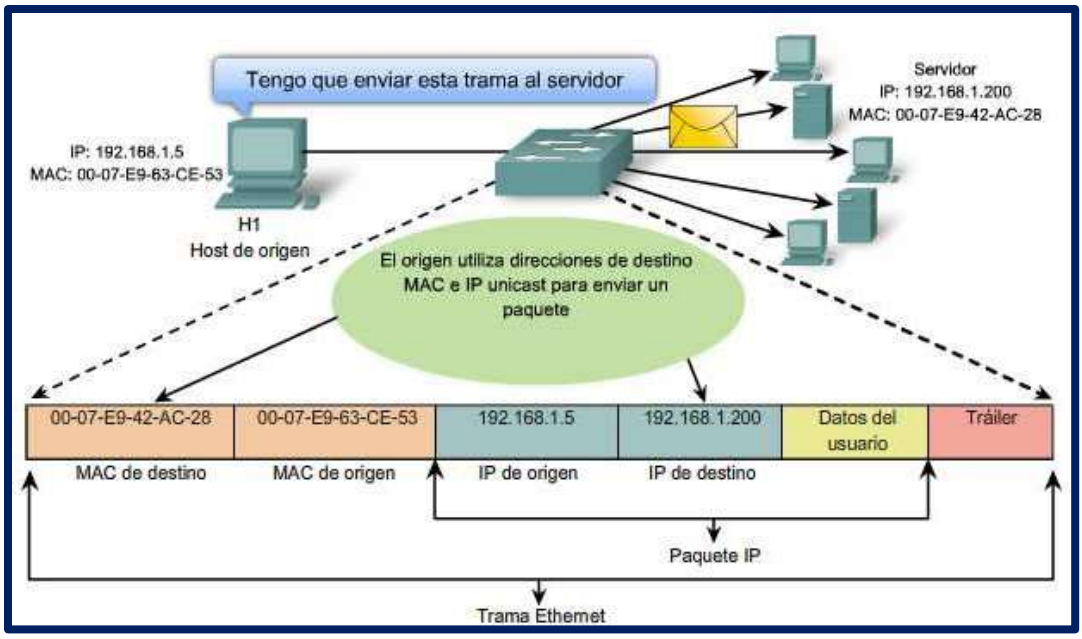
Los formatos de las direcciones pueden ser similares a 00-05-9A-3C-78-00, 00:05:9A:3C:78:00 ó 0005.9A3C.7800. Las direcciones MAC se asignan a estaciones de trabajo, servidores, impresoras, switches y routers (cualquier dispositivo que pueda originar o recibir datos en la red).

Una herramienta útil para analizar la dirección MAC de nuestro ordenador es ipconfig /all (Windows) o ifconfig (Linux). En el gráfico, observa la dirección MAC de este ordenador. Inténtalo esto en tu propio ordenador.

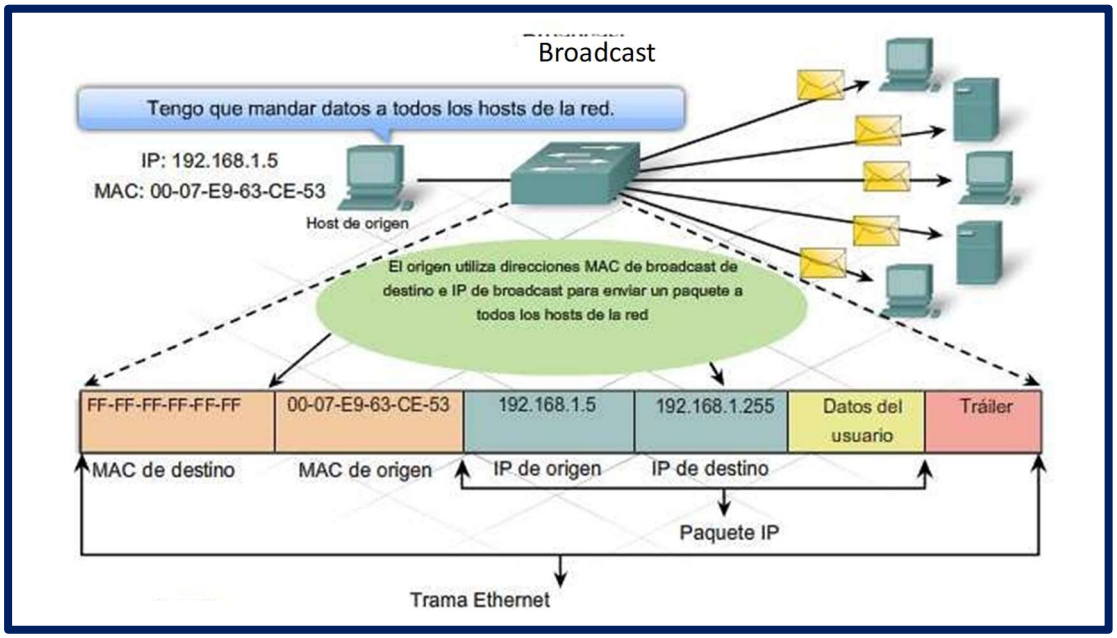
```
C:\>ipconfig /all
Ethernet adapter Network Connection:
        Connection-specific DNS Suffix: example.com
        Description . . . . . . . . . . . : Intel(R) PRO/Wireless 3945ABG Network
Connection
        Physical Address. . . . . . . . . : 00-18-DE-C7-F3-FB
        Dhcp Enabled. . . . . . . . . . . : Yes
        Autoconfiguration Enabled . . . . : Yes
        IP Address. . . . . . . . . . . . : 10.2.3.4
        Subnet Mask . . . . . . . . . . . : 255.255.255.0
        Default Gateway . . . . . . . . . : 10.2.3.254
        DHCP Server . . . . . . . . . . . : 10.2.3.69
        DNS Servers . . . . . . . . . . . : 192.168.226.120
        Lease Obtained. . . . . . . . . . : Thursday, May 03, 2007 3:47:51 PM
        Lease Expires . . . . . . . . . . : Friday, May 04, 2007 6:57:11 AM
C:\>
```

En Ethernet se utilizan distintas direcciones MAC para la Capa 2 (OSI): comunicaciones unicast, multicast y broadcast.

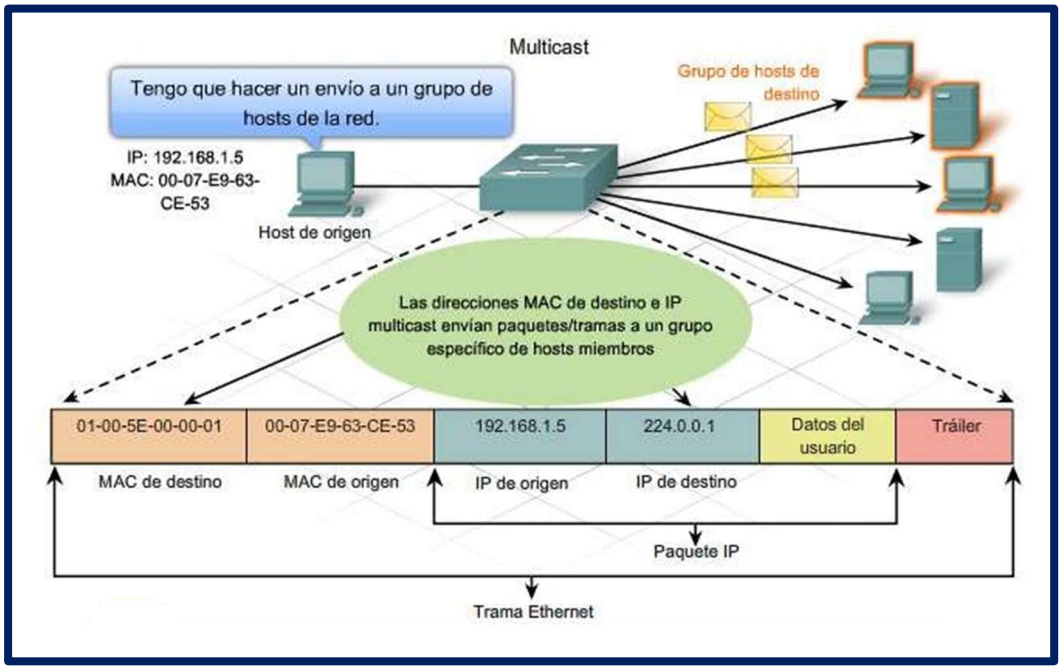
Unicast. Una dirección MAC unicast es la dirección exclusiva que se utiliza cuando se envía una trama desde un dispositivo de transmisión único hacia un dispositivo de destino único.
En el ejemplo que se muestra en la figura, un host con una dirección IP 192.168.1.5 (origen) solicita una página web del servidor en la dirección IP 192.168.1.200. Para que se pueda enviar y recibir un paquete unicast, el encabezado del paquete IP debe contener una dirección IP de destino. Además, el encabezado de la trama de Ethernet también debe contener una dirección MAC de destino correspondiente. Las direcciones IP y MAC se combinan para la entrega de datos a un host de destino específico.



Broadcast. Con broadcast, el paquete contiene una dirección IP de destino con todos unos (1) en la porción de host. Esta numeración en la dirección significa que todos los hosts de esa red local (dominio de broadcast) recibirán y procesarán el paquete. Una gran cantidad de protocolos de red utilizan broadcast, como el Protocolo de configuración dinámica de host (DHCP) y el Protocolo de resolución de direcciones (ARP).
Como se muestra en la figura, una dirección IP de broadcast para una red requiere una dirección MAC de broadcast correspondiente en la trama de Ethernet. En redes Ethernet, la dirección MAC de broadcast contiene 48 unos que se muestran como el hexadecimal FF-FF-FF-FF-FF-FF.

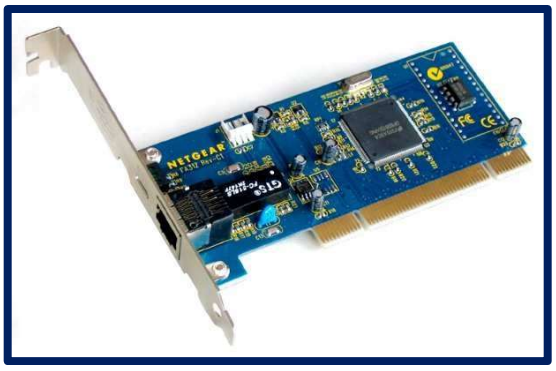


Multicast. Recuerda que las direcciones multicast le permiten a un dispositivo de origen enviar un paquete a un grupo de dispositivos. Una dirección IP de grupo multicast se asigna a los dispositivos que pertenecen a un grupo multicast. El intervalo de direcciones multicast es de 224.0.0.0 a 239.255.255.255. Debido a que las direcciones multicast representan un grupo de direcciones (a veces denominado un grupo de hosts), sólo pueden utilizarse como el destino de un paquete. El origen siempre tendrá una dirección unicast.
Ejemplos de dónde se utilizarían las direcciones multicast serían el juego remoto, en el que varios jugadores se conectan de manera remota pero juegan el mismo juego, y el aprendizaje a distancia a través de videoconferencia, en el que varios estudiantes se conectan a la misma clase.
Al igual que con las direcciones unicast y de broadcast, la dirección IP multicast requiere una dirección MAC multicast correspondiente para poder enviar tramas en una red local. La dirección MAC multicast es un valor especial que comienza con 01-00-5E en hexadecimal. El valor termina con la conversión de los 23 bits inferiores de la dirección IP del grupo multicast en los 6 caracteres hexadecimales restantes de la dirección de Ethernet. El bit restante en la dirección MAC es siempre "0".



NIC (NETWORK INTERFACE CARD)

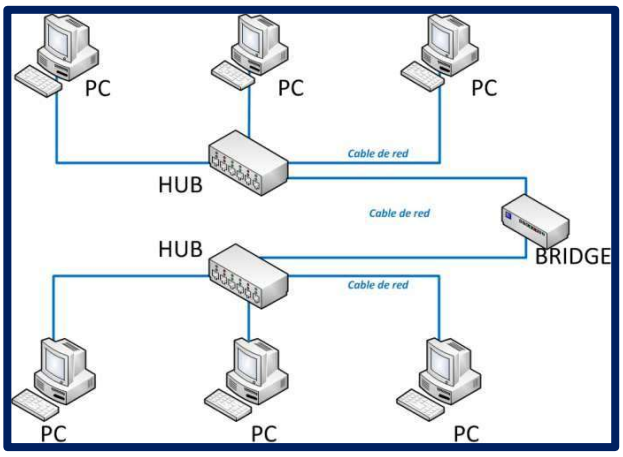
Tarjeta de Interfaz de Red, es el elemento que permitirá la conexión del PC a la red, al medio físico. Existen diferentes tipos en función de la arquitectura o cableado de red que se utilice (tendremos adaptadores para redes Ethernet, Token Ring, inalámbricas, etc.)



PUENTES (BRIDGES)

Es el dispositivo encargado de conectar a nivel de enlace redes con topologías y protocolos diferentes. Como su nombre indica, es un puente o salto a la otra red.

Es un dispositivo que está formando por al menos dos interfaces diferentes, una por cada tipo de red que conecta, por ejemplo, si tenemos una estructura de red LAN con cable par trenzado y otra con cable coaxial, tendrá como mínimo un conector RJ45 y BNC hembras.



Además, este dispositivo no solo se encarga de conectar redes diferentes a nivel de enlace, controla el tráfico de red de forma que no deja pasar a través de él cualquier paquete que no esté remitido a la otra red, es decir, solo "atraviesan el puente" aquellos paquetes cuyo destino sea un ordenador de la otra LAN, a diferencia de los repetidores que retransmitían la información a todos.

PUNTO DE ACCESO INALÁMBRICO (AP, Access Point)

Se encarga de interconectar dispositivos inalámbricos para formar una red inalámbrica. Normalmente un AP tiene una serie de puertos RJ45 que le permiten conectar con la red cableada pudiendo enviarse información desde la red inalámbrica a la cableada.

Básicamente un punto de acceso es un repetidor, ya que en el momento que recibe un dato lo almacena y lo transmite a todos los puestos inalámbricos y cableados.

CONMUTADORES (SWITCH)

Conectan redes a nivel de enlace de datos pero a diferencia de los puentes estas redes deben cumplir los mismos protocolos. Se usan conmutadores para segmentar la red y mejorar su rendimiento.

Un switch es selectivo de forma que solo enviará la información a través del puerto por el que se llega al PC receptor de esta. Así, si la tasa de transferencia de la red es de 10 Mbps, todos los puertos disfrutarán de esta velocidad porque en el mismo instante la información solo estará transmitiéndose por uno de ellos.

Normalmente cuando estudiamos los switch decimos que son “inteligentes”, la verdad es que aprenden en función de las peticiones de envío que se realicen. Cuando un equipo en la red quiere transmitir, el switch observa la dirección IP destino del paquete a enviar. En ese momento realiza una petición ARP7 (Protocolo de resolución de direcciones) por la que solicita que se busque la dirección MAC asociada a esta dirección IP (ya que es un dispositivo de nivel de enlace). Finalmente, el dispositivo configura una tabla en la que encontraremos (MAC del puerto del switch) -- (MAC del NIC del PC con dirección IP buscada), de forma que, en los próximos envíos a esa dirección, el switch ya habrá aprendido adonde transmitir los datos.

3. Dispositivos hardware de nivel de red

Estos dispositivos trabajan con direcciones IP, 32 bits agrupados en 4 números decimales. Desempeñan las funciones que se indican en el nivel de red.

ENCAMINADORES O ROUTERS

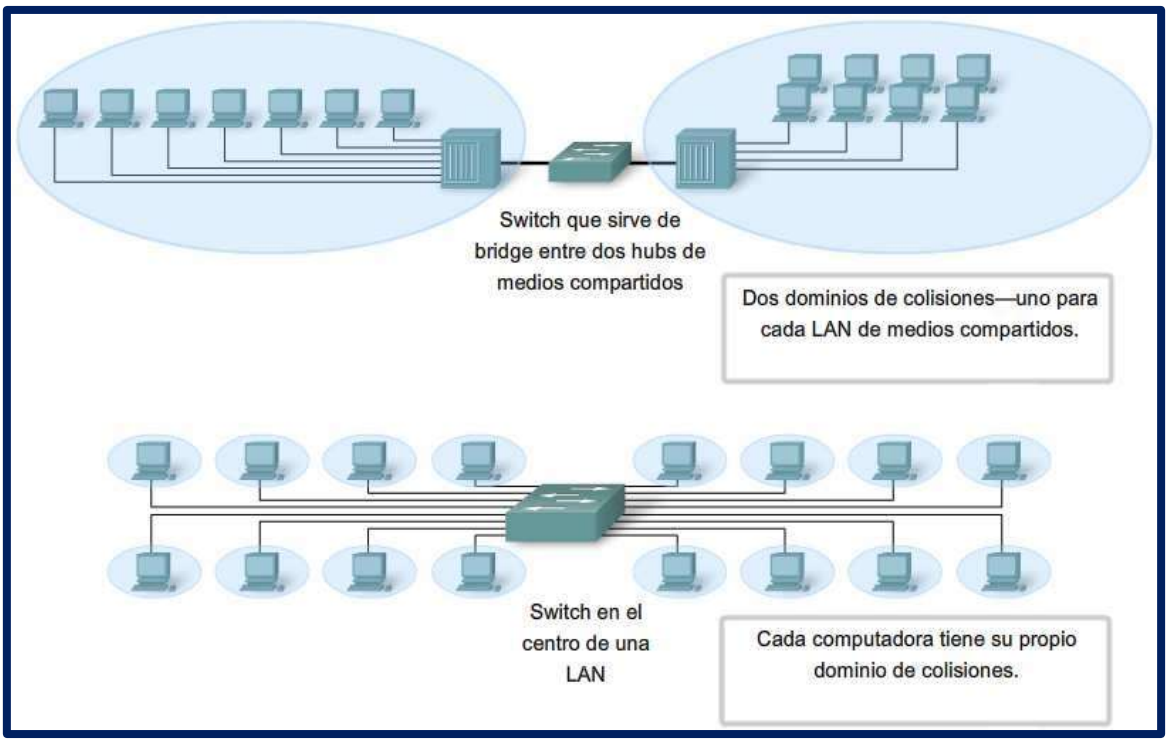
Estos dispositivos conectan la red al resto de redes dejando sólo pasar la información a través de ellos cuando va dirigida a un equipo con dirección IP de una red diferente a la del equipo emisor. Además, a la hora de transmitir la información a otra red se encargan de localizar la ruta más óptima, el camino más corto y seguro por el que puede ser enviada esta.

NOTA. Un dominio de colisión es el área o medio de transmisión compartido donde un conjunto de equipos se encuentra conectado formando una red, de forma que si dos equipos transmiten al mismo tiempo, se produce una colisión entre las tramas producidas. Todos los equipos unidos mediante dispositivos de nivel físico (cable, patch panel, transceiver, repetidor o hub) forman parte del mismo dominio de colisión. Un dominio de colisión también se denomina segmento de red.

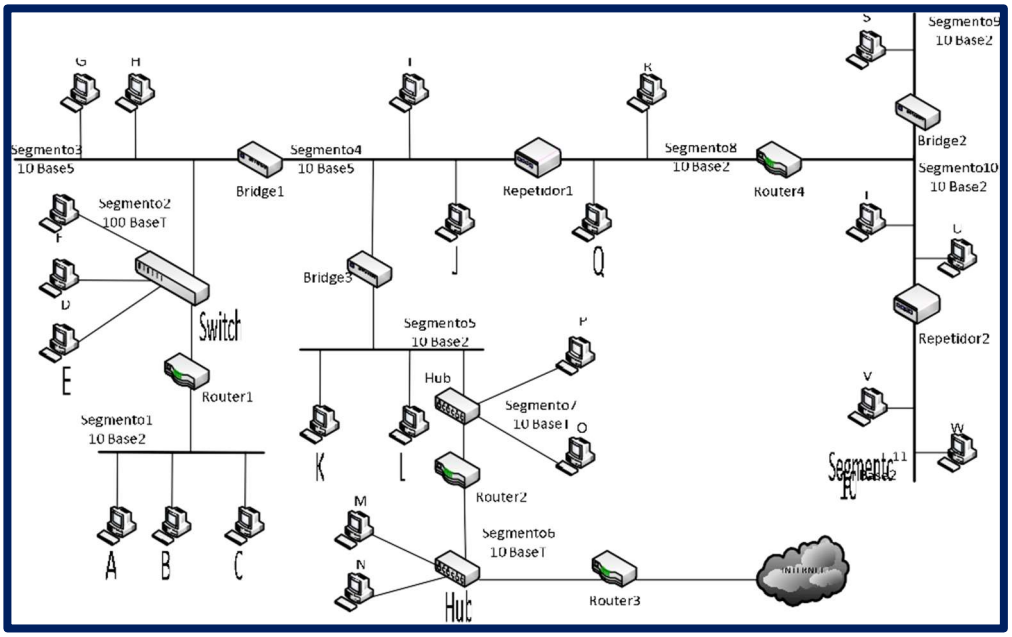
Existe otro concepto conocido como dominio de broadcast o difusión que no debe confundirse con dominio de colisión. Un dominio de difusión es un área o zona donde un grupo de dispositivos está conectado formando una red de manera que cuando alguno de ellos genera una trama de difusión o broadcast (trama dirigida a todos), todos los equipos reciben dicha trama. Visto desde otra perspectiva un dominio de difusión es un área en una red en la que cualquier dispositivo conectado puede trasmitir directamente a cualquier otro en el dominio sin precisar de ningún dispositivo de encaminamiento.

El dominio de colisión y de difusión son dos conceptos muy importantes y muy utilizados para definir la funcionalidad de los dispositivos de conexión de red, como repetidores y concentradores (hub) que conectan dos segmentos de cable, formando un único dominio de colisión; puentes y conmutadores (switch), que dividen la red en distintos dominios de colisión y enrutadores (router), que segmentan tanto los dominios de colisión como de difusión (broadcast).

El dominio de colisión y el de broadcast no siempre coinciden en una red. Los dominios de colisión están delimitados por switches, mientras que los dominios de broadcast se encuentran normalmente delimitados por routers, debido a que los routers no reenvían tramas de broadcast.



Una empresa presenta el siguiente diseño de red.



¿Qué es un dominio de colisión?

Un dominio de colisión es un segmento de red donde las señales de datos pueden interferir entre sí porque comparten el mismo medio físico. Cuando dos dispositivos dentro de un mismo dominio intentan transmitir datos al mismo tiempo, ocurre una colisión.

Puntos clave para identificar dominios de colisión en la imagen:

- Busca los hubs y agrupa los dispositivos conectados a ellos en un solo dominio de colisión.
- Para los switches, asigna un dominio de colisión a cada dispositivo conectado a un puerto, y recuerda incluir los enlaces que conectan switches entre sí.
- Los routers no afectan los dominios de colisión; actúan en un nivel diferente.

Cómo identificar dominios de colisión en la imagen:

1. **Hubs (concentradores):** Los hubs no aíslan el tráfico entre los dispositivos conectados a ellos, por lo que todos los dispositivos conectados al mismo hub comparten un único dominio de colisión.
   Ejemplo en la imagen: Si un hub central conecta 4 PCs, todos ellos están en el mismo dominio de colisión.
2. **Switches (conmutadores):** Los switches separan dominios de colisión. Cada puerto del switch constituye un dominio independiente.
   Esto significa que cada dispositivo conectado directamente a un puerto de un switch está en su propio dominio de colisión.
   Ejemplo en la imagen: Si un switch tiene 8 puertos y hay un dispositivo conectado a cada puerto, entonces hay 8 dominios de colisión.
3. **Enlaces entre switches:** Los enlaces entre switches también forman dominios de colisión propios. Por ejemplo, si dos switches están conectados mediante un cable Ethernet, ese enlace será un dominio de colisión separado.

Ejemplo aplicado:

Supongamos que hay:

- Un hub con 6 PCs conectados → 1 dominio de colisión.
- Un switch con 8 PCs conectados → 8 dominios de colisión.
- Otro switch con 4 PCs conectados → 4 dominios de colisión.
- Un enlace entre los dos switches → 1 dominio de colisión.

Total: 1 + 8+ 4 + 1 = 14 dominios de colisión.

¿Qué es un dominio de broadcast?

Un dominio de broadcast es un segmento de red donde los paquetes de tipo *broadcast* (dirigidos a "todos los dispositivos") pueden ser recibidos por todos los dispositivos dentro de ese segmento.

Cómo identificar dominios de broadcast en la imagen:

1. Hubs (concentradores)

- Todos los dispositivos conectados a un mismo hub están en el **mismo dominio de broadcast**.
- Esto se debe a que los hubs simplemente replican el tráfico recibido en un puerto a todos los demás puertos.

2. Switches (conmutadores)

- Todos los dispositivos conectados a un switch comparten el **mismo dominio de broadcast**, ya que los switches permiten que los paquetes *broadcast* se propaguen a todos los dispositivos conectados.

3. Routers

- Los routers dividen los dominios de broadcast. Cada interfaz del router crea un límite, y los dispositivos conectados a interfaces diferentes del router están en dominios de broadcast distintos.
- Por ejemplo, si un router conecta tres segmentos de red, cada uno de esos segmentos es un dominio de broadcast separado.

Cálculo total de dominios de broadcast en la imagen

Para contar los dominios de broadcast:

1. Identificar cuántos routers hay y cuántas interfaces utilizan.
2. Dividir la red en segmentos, donde cada segmento conectado a una interfaz de un router será un dominio de broadcast único.

Ejemplo aplicado a la imagen:

1. **Hubs y switches:**
    - Si hay dispositivos conectados a un hub o switch, están en el mismo dominio de broadcast hasta que un router lo divida.
    - Ejemplo: Si 10 PCs están conectados al mismo switch, todos están en el mismo dominio de broadcast.
2. **Routers:**
    - Cada interfaz de un router define un dominio de broadcast separado. Por ejemplo, si un router conecta a tres segmentos diferentes de la red, entonces esos tres segmentos forman tres dominios de broadcast independientes.
3. **Enlaces entre switches:**
    - Los enlaces entre switches no dividen el dominio de broadcast, ya que los paquetes *broadcast* pueden viajar entre switches.

Análisis específico:

Supongamos que:

- Hay 2 routers en la red con un total de 4 interfaces activas (2 por cada router).
- Los dispositivos conectados a switches y hubs forman grupos no separados por routers.

Cálculo:

- Cada interfaz de un router crea un dominio de broadcast. Si hay 4 interfaces activas, hay **4 dominios de broadcast**.
- Todos los dispositivos conectados a un mismo switch o hub sin intervención de routers están dentro de uno de estos dominios de broadcast.

Representación de los dominios de broadcast en la imagen

1. **Dibuja cajas o zonas alrededor de los grupos de dispositivos** que comparten el mismo dominio de broadcast (segmentos conectados a un router forman zonas separadas).
2. Usa colores diferentes para identificar qué dispositivos pertenecen a qué dominio.
3. Resalta los routers como límites entre dominios.

Resumen

1. Un dominio de broadcast incluye todos los dispositivos conectados a un switch o hub **hasta que un router los separe**.
2. Para contar los dominios, suma el número de interfaces activas de los routers.
3. Total de dominios de broadcast = Número de segmentos divididos por routers.

8. REDES DE ÁREA LOCAL

Existen diferentes tipos de redes de área local definidas por el IEEE con el nombre 8028. 802.3 y 802.11 son los estándares más usados actualmente.

9. MONTAJE FÍSICO DE UNA RED CABLEADA

Antes de comenzar con el montaje de una red cableada debemos planificar ésta, teniendo en cuenta el número de equipos que tendrá la red, las distancias entre estos equipos, si además vamos a contratar un Proveedor de Servicios de Internet (ISP), etc.

Así, se aconseja que en un primer momento y sobre papel (si puede ser sobre los planos de la planta a cablear) se realice un esquema de la distribución de los equipos de red. En función del número de PCs el conmutador variará ya que deberá tener mayor o menor número de puertos, y si los equipos están alejados probablemente necesitaremos más de un switch en nuestra configuración.

10. PROTOCOLO IP (NIVEL DE INTERNET EN TCP/IP)

En esta capa de la arquitectura TCP/IP se lleva a cabo el direccionamiento y encaminamiento de la información, siendo el protocolo IP el encargado de ello. A este nivel trabajamos con unidades de datos llamados datagramas que siguen el formato especificado en el protocolo IP.

- **Direccionamiento.** Todo elemento en la red es claramente diferenciado mediante una dirección IP que identifica la red a la que pertenece y el equipo concreto dentro de esta.
- **Encaminamiento.** Todo elemento en la red es encaminado, conducido a su destino, con la ayuda de componentes que mantienen tablas de direcciones con caminos alternativos.

La versión más utilizada del **protocolo IP es la 4 (IPv4)** que sigue predominando, aunque la IPv6 ya está desarrollada.

10.1. DIRECCIONAMIENTO IP

El direccionamiento IP trata la forma en la que el protocolo IP identifica a los nodos de la red. Todo nodo en la red posee una única dirección IP. En realidad, esto no es del todo exacto, ya que un único nodo podría tener varias direcciones IP si tiene instaladas varias interfaces de red (o tarjetas de red), de forma que es más acertado decir que una dirección IP es única por cada interfaz que exista en la red.

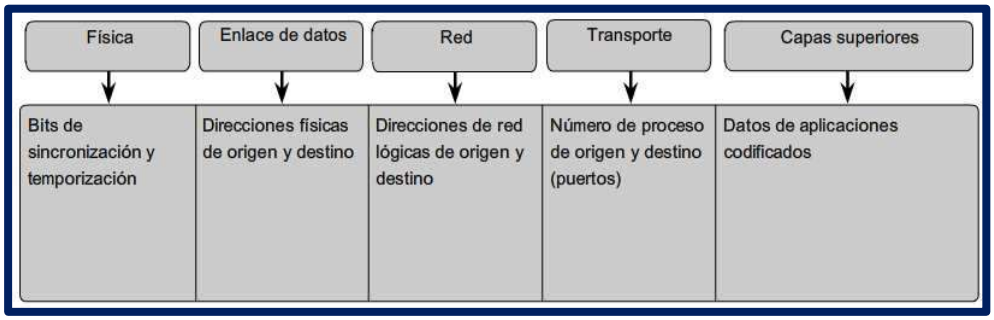
Las direcciones de red pueden ser:

- **Unicast.** Referencian una única interfaz de red. Las direcciones IP unicast son las que usamos normalmente en el envío de información, ya que ésta sólo va dirigida a un único componente de la red.
- **Multicast.** Una dirección IP multicast referencia varias interfaces en una red, de forma que, si enviamos un paquete con una dirección multicast, este paquete llegará a más de una interfaz de red.
- **Broadcast.** Dirección de referencia todos los equipos de una red.

Direccionamiento en la red

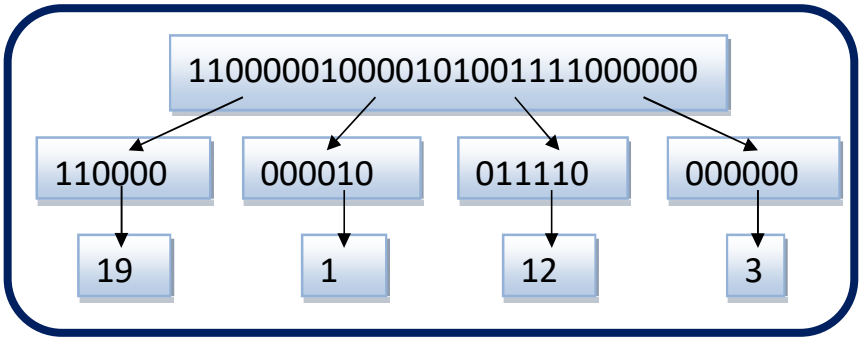
El modelo OSI describe los procesos de codificación, formateo, segmentación y encapsulación de datos para transmitir por la red. Un flujo de datos que se envía desde un origen hasta un destino se puede dividir en partes y entrelazar con los mensajes que viajan desde otros hosts hacia otros destinos. Miles de millones de estas partes de información viajan por una red en cualquier momento. Es muy importante que cada parte de los datos contenga suficiente información de identificación para llegar al destino correcto.

Existen varios tipos de direcciones que deben incluirse para entregar satisfactoriamente los datos desde una aplicación de origen que se ejecuta en un host hasta la aplicación de destino correcta que se ejecuta en otro. Al utilizar el modelo OSI como guía, se pueden observar las distintas direcciones e identificadores necesarios en cada capa.



FORMATO DE UNA DIRECCIÓN IPv4

Una dirección IPv4 está compuesta por 32 bits, agrupados de 8 en 8. Cada grupo de 8 bits genera un número decimal que va de 0 a 255.

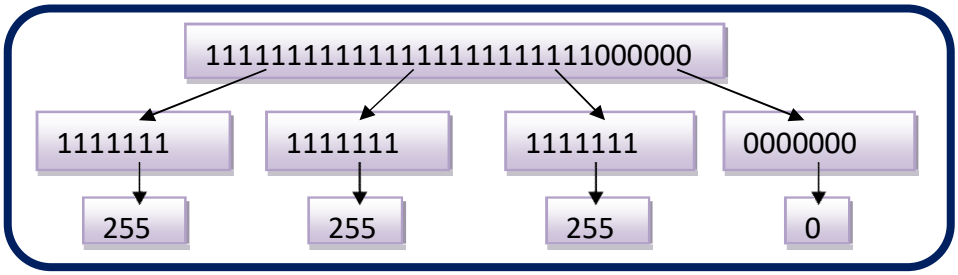


En una dirección IPv4 se diferencian dos partes:

- **Identificador de red.** Es la parte de la dirección IP que identifica la red donde se encuentra el equipo.
- **Identificador de host.** Nombre del PC en la red.

MÁSCARA DE SUBRED IPv4

La máscara de subred se usa para diferenciar los bits de red de los de host en una dirección IPv4. La máscara está formada por 32 bits de los que aquellos que identifiquen red tendrán valor 1 y aquellos que identifiquen host valor 0. Estos 32 bits se agrupan de 8 en 8 al igual que en una dirección IP.

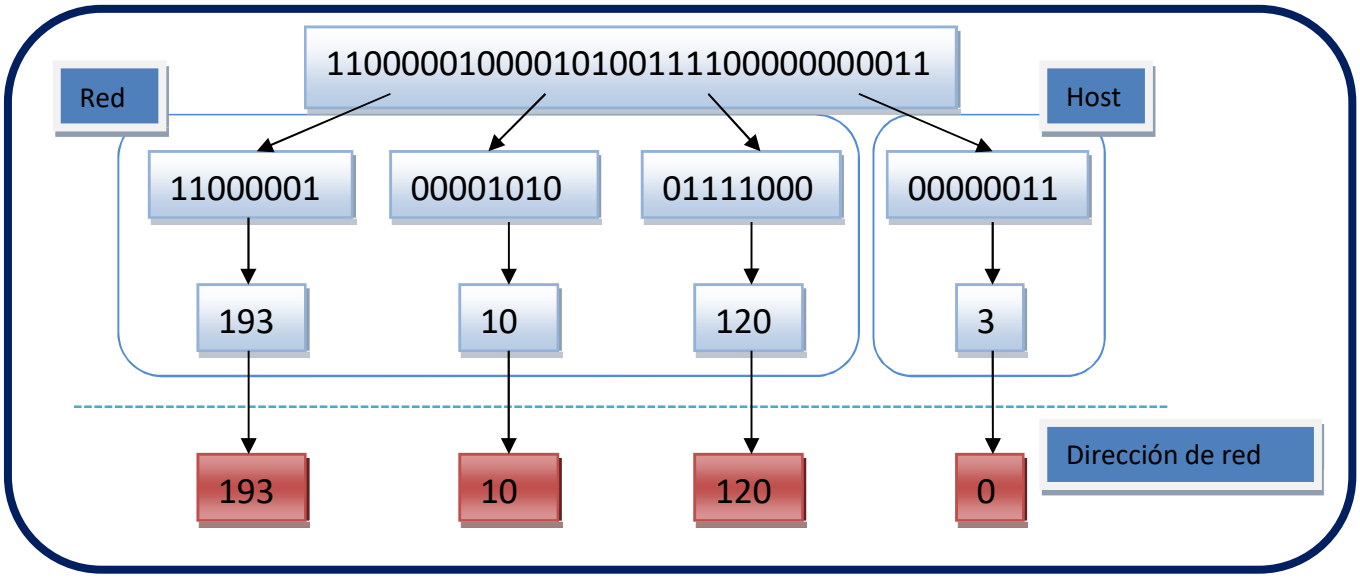


Máscara de red. 24 primeros bits de red y 8 últimos bits de host.

Una máscara de red puede también expresarse usando la notación CIDR (Classless InterDomain Routing). Esta notación consiste en agregar un sufijo a la dirección IP indicando el nº de bits que se usan para identificar a la red, teniendo en cuenta que los bits de red empiezan a contar de izquierda a derecha de la dirección IP.
Ejemplo de notación CIDR: **193.10.120.3/24** (la máscara sería 255.255.255.0).

DIRECCIÓN DE RED IPv4

La dirección de red se obtiene poniendo a cero todos los bits de host de una dirección IP. Así, si mi dirección IP es 193.10.120.3 y sé que los últimos 8 bits representan host, en una máscara 255.255.255.0:



Ejemplo de dirección de red.

CLASES DE DIRECCIONES IPv4

El número de bits que identifican la red en una dirección IP es variable. Las clases nos ayudan a averiguar el número de bits que la dirección dedica a red y a host. Las direcciones IP pueden ser de:

- **Clase A.**
  - → Usan los 8 primeros bits para identificar red y 24 restantes para identificar host.
  - → El primer bit de la dirección comienza con el valor 0.
  - → Estas direcciones se encontrarán en el intervalo 0.0.0.0 a 127.255.255.255.
  - → La máscara de red para estas direcciones es 255.0.0.0.
- **Clase B.**
  - → Usan los 16 primeros bits para identificar red y los 16 restantes para identificar host.
  - → Los dos primeros bits adoptan el valor 10.
  - → Estas direcciones se encontrarán en el intervalo 128.0.0.0 a 191.255.255.255.
  - → La máscara de red para estas direcciones es 255.255.0.0.
- **Clase C.**
  - → Usan los 24 primeros bits para identificar red y los 8 restantes para identificar host.
  - → Los tres primeros bits siguen la secuencia 110.
  - → Estas direcciones se encontrarán en el intervalo 192.0.0.0 a 223.255.255.255.
  - → La máscara de red para estas direcciones es 255.255.255.0.
- **Clase D.**
  - → Son direcciones IP destinadas a multicasting.
  - → Sus primeros bits comienzan con la combinación 1110.
  - → El intervalo de direcciones IP para esta clase es 224.0.0.0 a 239.255.255.255.
- **Clase E.**
  - → Direcciones IP reservadas para uso en investigaciones.
  - → Sus primeros bits comienzan con la secuencia 11110.
  - → El intervalo de direcciones IP para esta clase es 240.0.0.0 a 255.255.255.255.

NOTA: En las clases D y E debido a sus peculiaridades no se distinguen partes, no se diferencian entre bits de red y bits de host (no tienen máscaras).

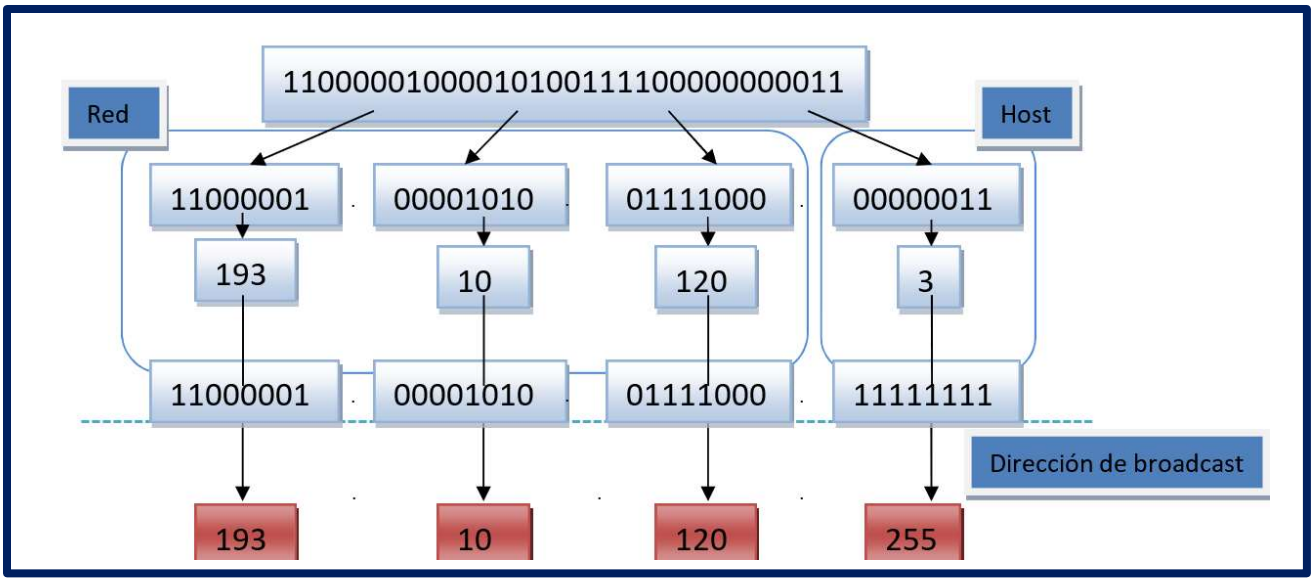
DIRECCIONES IPv4 PÚBLICAS Y PRIVADAS

Debido a que el espacio de direcciones IP es limitado y sobre todo en IPv4 casi agotado, se plantea una división de las direcciones entre IP públicas y privadas.

- **Direcciones IP públicas.** Son direcciones IP únicas e irrepetibles en Internet.
- **Direcciones IP privadas.** Existen rangos de direcciones IP que no se utilizan a nivel público, ningún ordenador en internet puede adoptar la IP, sino que se dejan para uso privado en redes internas, de forma que pueden existir varias empresas que usen para configurar su red la misma dirección IP. Existen direcciones IP privadas de las tres primeras clases:
  - → **Clase A** rango de direcciones IP desde 10.0.0.0 a 10.255.255.255.
  - → **Clase B** rango de direcciones IP desde 172.16.0.0 a 172.31.255.255.
  - → **Clase C** rango de direcciones IP desde 192.168.0.0 a 192.168.255.255.

DIRECCONES IP INTERESANTES

- **Dirección IP de la puerta de enlace.** En definitiva, el objeto del protocolo IP es conseguir que la información sea transmitida, pasando por el encaminador que detectará en qué red se encuentra el paquete a enviar. Así, la puerta de enlace o gateway es la dirección IP del encaminador (router) del sistema. La puerta de enlace puede ser cualquiera de las direcciones IP de un rango, normalmente se suele usar la primera dirección IP del rango o la última.
- **Dirección de broadcast.** Dirección de multidifusión por la que se enviará un paquete a todos los nodos de la red. La dirección de broadcast de una red se consigue poniendo a 1 todos los bits de host.
- **Dirección de bucle local.** Es una dirección de red que se usa para comprobación de las propias interfaces de red. Esta dirección de red de clase A es 127.0.0.0. Normalmente, las comprobaciones se realizan usando la IP 127.0.0.1 pero cualquier otra de esta red es válida, por ejemplo 127.10.10.1. No podemos usar en ninguna de nuestras redes esta dirección de red.



CONFIGURACIÓN DEL DIRECCIONAMIENTO IP EN UNA RED

El paso posterior al montaje de una red es su configuración. Una vez instalados todos sus componentes debemos ir puesto por puesto (en caso de no disponer de un DHCP) e ir indicando una serie de datos que permitirán que ese host pueda acceder a la red.

Así, para configurar una red debemos:

- Disponer de una dirección de red.
- Máscara de red.
- Dirección de la puerta de enlace (dirección que asignaremos al router para el acceso a Internet)
- Dirección de broadcast.
- Rango de direcciones IP que podemos usar para asignar a cada host.

Normalmente, cuando tengamos una LAN esta se configurará usando alguna de las direcciones IP privadas estudiadas. Será el modem cable, modem ADSL, etc., que nos proporciona el Proveedor de Servicio de Internet (ISP) que hayamos contratado para la conexión a Internet el que disponga de una IP pública.

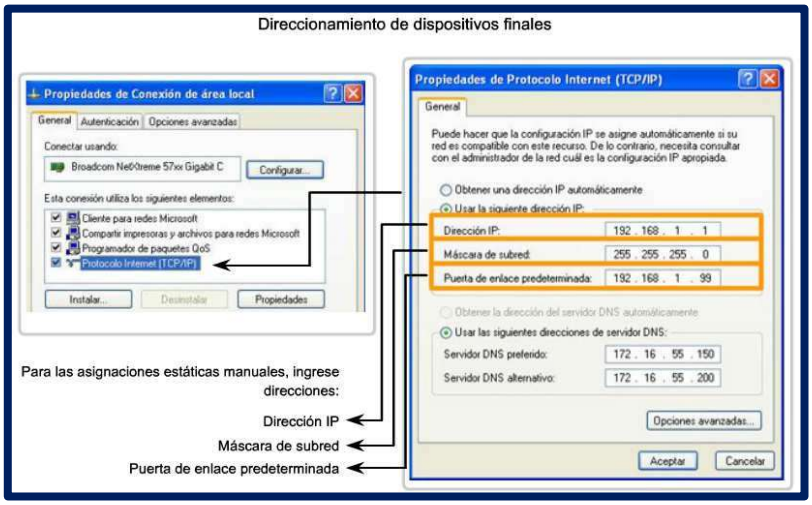
Direcciones para dispositivos de usuario

En la mayoría de las redes de datos, la mayor población de hosts incluye dispositivos finales como PC, teléfonos IP, impresoras y asistentes digitales personales (PDA). Debido a que esta población representa la mayor cantidad de dispositivos en una red, debe asignarse la mayor cantidad de direcciones a estos hosts.

Las direcciones IP pueden asignarse de manera estática o dinámica.

Asignación estática de direcciones

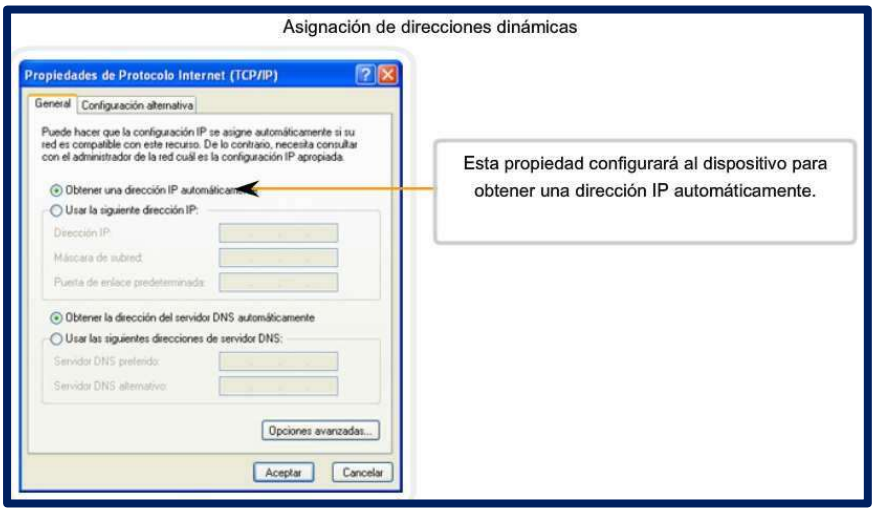
Con una asignación estática, el administrador de red debe configurar manualmente la información de red para un host, como se muestra en la figura. Como mínimo, esto implica introducir la dirección IP del host, la máscara de subred y el gateway por defecto.Las direcciones estáticas tienen algunas ventajas en comparación con las direcciones dinámicas. Por ejemplo, resultan útiles para impresoras, servidores y otros dispositivos de red que deben ser accesibles a los clientes de la red. Si los hosts normalmente acceden a un servidor en una dirección IP en particular, esto provocaría problemas si se cambiara esa dirección. Además, la asignación estática de información de direccionamiento puede proporcionar un mayor control de los recursos de red. Sin embargo, puede llevar mucho tiempo introducir la información en cada host.



Al utilizar direccionamiento IP estático, es necesario mantener una lista precisa de las direcciones IP asignadas a cada dispositivo. Éstas son direcciones permanentes y normalmente no vuelven a utilizarse.

Asignación dinámica de direcciones

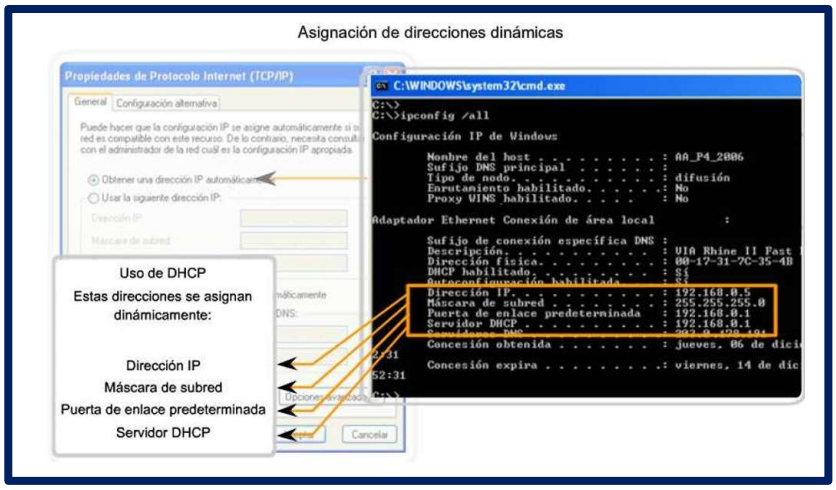
Debido a los desafíos asociados con la administración de direcciones estáticas, los dispositivos de usuarios finales a menudo poseen direcciones que se asignan en forma dinámica utilizando el protocolo de configuración dinámica de host (DHCP), como se muestra en la figura.



El DHCP permite la asignación automática de información de direccionamiento, como una dirección IP, una máscara de subred, un gateway predeterminado y otra información de configuración. La configuración del servidor DHCP requiere definir un bloque de direcciones, denominado pool de direcciones, para asignarlo a los clientes DHCP en una red. Las direcciones asignadas a este pool deben ser planificadas de manera que se excluyan las direcciones utilizadas para otros tipos de dispositivos.

Generalmente, el DHCP es el método que se prefiere para asignar direcciones IP a los hosts de grandes redes, dado que reduce la carga para al personal de soporte de la red y prácticamente elimina los errores de entrada.

Otro beneficio de DHCP es que no se asigna de manera permanente una dirección a un host, sino que sólo se la "alquila" durante un tiempo. Si el host se apaga o se desconecta de la red, la dirección regresa al pool para volver a utilizarse. Esta función es muy útil para los usuarios móviles que entran y salen de la red.

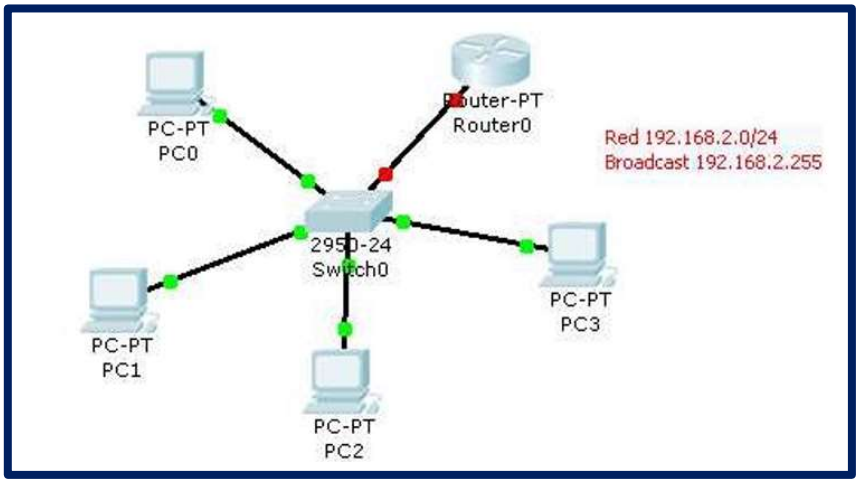


EJEMPLO PRÁCTICO 1

Imaginemos que debemos configurar una red en la que nos indican el número de ordenadores de la misma. En el ejemplo debemos configurar una red compuesta por unos 50 ordenadores usando direcciones IP privadas. ¿Cómo debo proceder?

1. Antes de nada y para desaprovechar el menor número de direcciones IP posible, nos haremos la siguiente pregunta: ¿Qué clase de dirección IP necesito?
   → Una clase A usa 24 bits para referir host con lo que cada red de clase A tendrá un total de 2^{24} PCs como máximo; mi red solo necesita 50.
   → Una clase B puede soportar en cada red 2^{16} PCs; sigue siendo un número demasiado elevado.
   → **Finalmente, una dirección de clase C, 2^8=256 ordenadores sería la opción correcta.**
2. Ya sabemos la clase de dirección IP que vamos a usar, ahora debemos escoger del rango de direcciones IP privadas de clase C la que queramos. Por ejemplo, vamos a usar la **dirección de red 192.168.2.0**. Tenemos un total de 256 direcciones IP en el rango 192.268.2.0 a 192.168.2.255.
3. La siguiente pregunta a resolver es ¿qué máscara de red tiene esta dirección IP? Al ser una clase C **su máscara por defecto es 255.255.255.0**.
4. **No debemos ajustarnos al número, debemos prever que en un futuro el número de host pueda aumentar a la hora de configurar la red.**
5. A continuación, debemos conocer el rango de direcciones IP que podemos utilizar para asignar a cada host. De las 256 direcciones IP del punto 2, la primera de ellas, 192.168.2.0 es la dirección de red y la última es la denominada **dirección de broadcast, 192.168.2.255**, **ninguna de estas puede ser asignada a un PC**, sea cual sea el número total de direcciones IP que tengamos, siempre tendremos que restar a este número dos, ya que entre ellas está la dirección de broadcast y la de red. Así, el número de **direcciones IP asignables siempre se averiguará con la siguiente fórmula 2^n-2**, siendo n el número de bits de host de la red. El rango de direcciones IP asignables será 192.168.2.1 - 192.168.2.254.
6. Del rango calculado en el punto 5, debemos **reservar una dirección para nuestro enrutador**, por ejemplo, optamos por el uso de la última dirección IP asignable. Así, nuestra IP de **puerta de enlace será 192.168.2.254** y el **rango de direcciones IP se verá modificado 192.168.2.1 - 192.168.2.253.**
7. A partir de aquí podemos agrupar las direcciones IP como queramos, en función de los dispositivos de red que tengamos, tipo, etc.
8. Seguidos estos pasos finalmente obtendremos una tabla con todos los datos necesarios para la configuración de la LAN, a falta de las direcciones DNS que nos la aporta el proveedor de internet. DNS (Domain Name Server) Servidor de Nombres de Dominio, que mantiene información de nombres de dominios y direcciones IP asociadas a ellos.

Dirección de red	Máscara de red	Dirección de broadcast	Dirección puerta enlace	Rango de direcciones IP
192.168.2.0	255.255.255.0	192.168.2.255	192.168.2.254	192.168.2.1/192.168.2.253

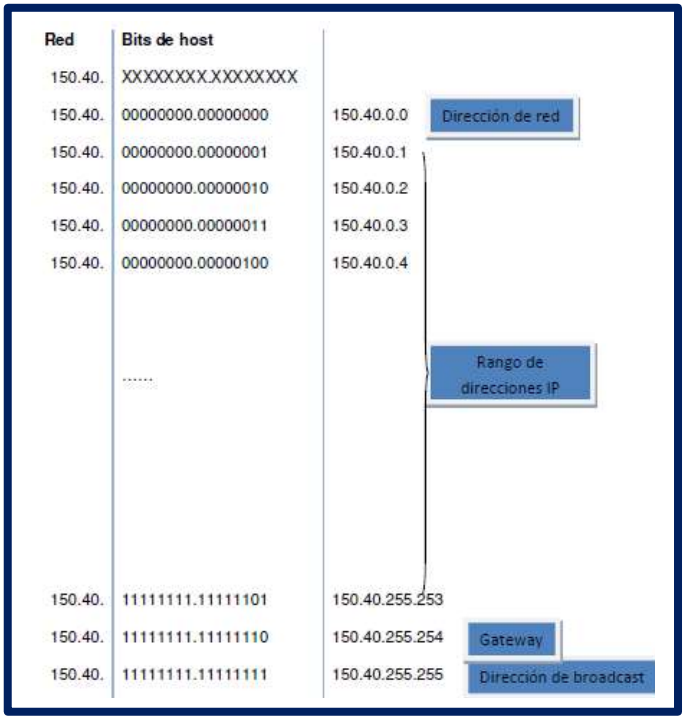


EJEMPLO PRÁCTICO 2

Imaginemos ahora que conocemos la dirección de red, y a partir de ella debemos extraer toda la información para configurar ésta. Como ejemplo, usaremos la dirección 150.40.0.0.

1. ¿Qué clase de dirección de red es 150.40.0.0? No sabemos su máscara, pero el primer número de la dirección nos dará información. Las direcciones tipo B tienen como primer número un valor incluido en el rango 128 a 191; 150 está en ese rango con lo que estamos frente a una **IP de clase B. La máscara de red es 255.255.0.0.**
2. ¿Cuál será la **dirección de broadcast**? Esta se consigue poniendo a 1 todos los bits de host, en una clase B, son los últimos 16 bits, así: 150.40.11111111.1111111115, **150.40.255.255.**
3. ¿Cuál será el rango de direcciones IP asignables? EI total de host a direccionar viene dado por 2^{16}-2 = 65534. El rango será 150.40.0.1 a 150.40.255.254**. Si la última de estas direcciones la usamos como gateway (150.40.255.254), tenemos el rango 150.40.0.1 a 150.40.255.253.**

Dirección de red	Máscara de red	Dirección de broadcast	Dirección de puerta de enlace	Rango de direcciones IP
150.40.0.0	255.255.0.0	150.40.255.255	150.40.255.254	150.40.0.1-150.40.255.253



Los dos primeros números expresados en decimal y los dos últimos en binario

11. SUBNETTING

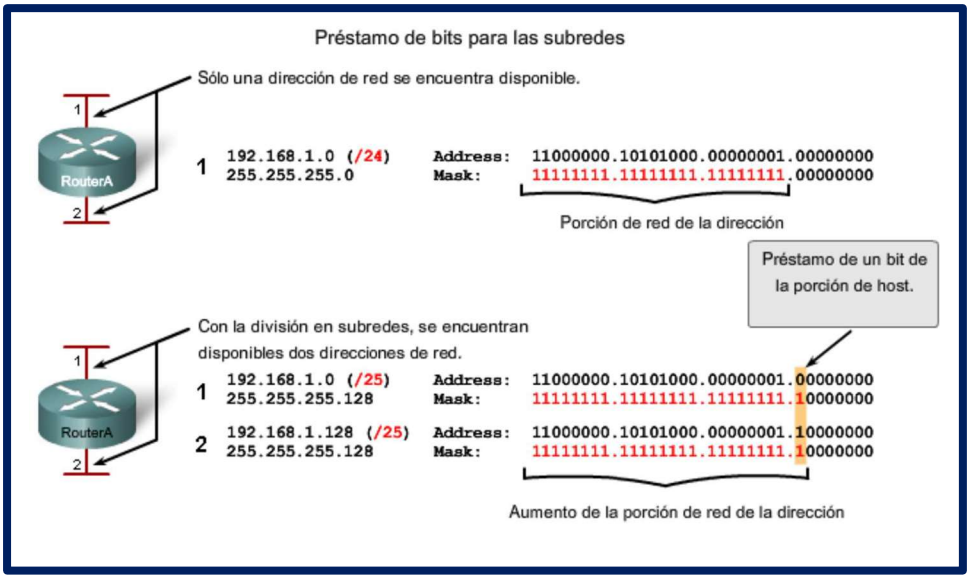
Las direcciones IPv4 están a punto de agotarse. Son tantas las personas que se conectan hoy día a la red que nos estamos quedando sin direcciones IPv4 para asignar. El estándar IPv6 está finalizado, pero apenas empieza a adoptarse y son escasos los usuarios que lo utilizan.

Una solución a este problema es el conocido subnetting. Esta técnica **divide una dirección de red dada en tantas redes como se necesite o sea posible, de forma que si necesitamos x direcciones de red vamos a tener solo una dividida x veces, estamos ahorrando x-1 direcciones de red que pueden ser aplicadas a otras redes**.

11.1. Principios de división en subredes

La división en subredes permite crear múltiples redes lógicas de un único bloque de direcciones. Como usamos un router para conectar estas redes, cada interfaz en un router debe tener un ID único de red. Cada nodo en ese enlace está en la misma red.

Creamos las subredes utilizando uno o más de los bits del host como bits de la red. Esto se hace ampliando la máscara para tomar prestados algunos de los bits de la porción de host de la dirección, a fin de crear bits de red adicionales. Cuantos más bits de host se usen, mayor será la cantidad de subredes que puedan definirse. Para cada bit que se toma prestado, se duplica la cantidad de subredes disponibles. Por ejemplo: si se toma prestado 1 bit, es posible definir 2 subredes. Si se toman prestados 2 bits, es posible tener 4 subredes. Sin embargo, con cada bit que se toma prestado, se dispone de menos direcciones host por subred.
El Router A en la figura posee dos interfaces para interconectar dos redes. Dado un bloque de direcciones 192.168.1.0 /24, se crearán dos subredes. Se toma prestado un bit de la porción de host utilizando una máscara de subred 255.255.255.128, en lugar de la máscara original 255.255.255.0. El bit más significativo del último octeto se usa para diferenciar dos subredes. Para una de las subredes, este bit es "0" y para la otra subred, este bit es "1".



Fórmula para calcular subredes
Se usa esta fórmula para calcular **la cantidad de subredes: 2^n** donde n corresponde a la cantidad de bits que se toman prestados.
En este ejemplo, el cálculo es así: $2^1 = 2$ subredes

→ **Cantidad de hosts**

Para calcular la cantidad de hosts por red, se usa la fórmula **$2^n - 2$** donde n corresponde a la cantidad de bits para hosts.
La aplicación de esta fórmula, ($2^7 - 2 = 126$) muestra que cada una de estas subredes puede tener 126 hosts.
En cada subred, observa el último octeto binario. Los valores de estos octetos para las dos redes son:

- Subred 1: **0**0000000 = 0
- Subred 2: **1**0000000 = 128

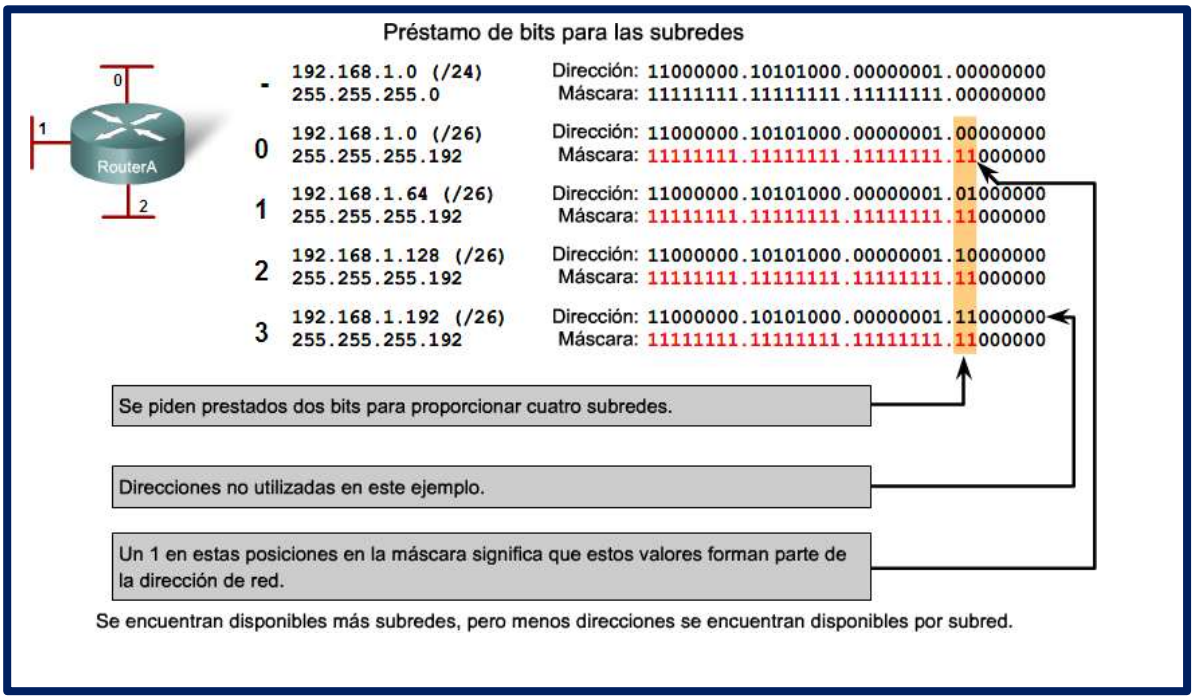
Observa la figura del esquema de direccionamiento para estas redes.

Esquema de direccionamiento: Ejemplo de 2 redes

Subred	Dirección de red	Rango de host	Dirección de broadcast
0	192.168.1.0/25	192.168.1.1 – 192.168.1.126	192.168.1.127
1	192.168.1.128/25	192.168.1.129 – 192.168.1.254	192.168.1.255

Ejemplo con 3 subredes

A continuación, piensa en una red que requiere tres subredes. Observa la figura.



Nuevamente, se comienza con el mismo bloque de direcciones 192.168.1.0 /24. Tomar prestado un solo bit proporcionará únicamente dos subredes. Para proveer más redes, se cambia la máscara de subred a 255.255.255.192 y se toman prestados dos bits. Esto proveerá cuatro subredes.

Calcula las subredes con esta fórmula: $2^2 = 4$ subredes

→ **Cantidad de hosts**

Para calcular la cantidad de hosts, comienza por examinar el último octeto. Observa estas subredes:

- Subred 0: 0 = **00**000000
- Subred 1: 64 = **01**000000
- Subred 2: 128 = **10**000000
- Subred 3: 192 = **11**000000

Aplica la fórmula de cálculo de host: $2^6 - 2 = 62$ hosts por subred

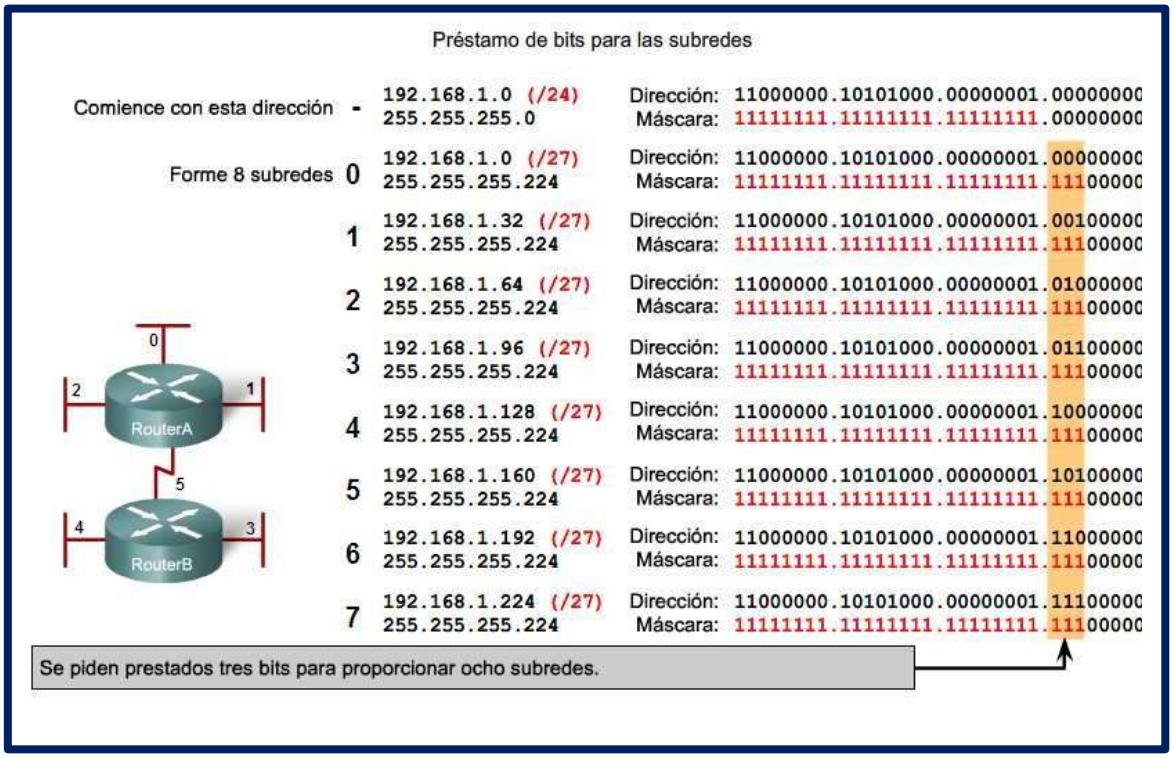
Observa la figura del esquema de direccionamiento para estas redes.

Esquema de direccionamiento: Ejemplo de 4 redes

Subred	Dirección de red	Rango de host	Dirección de broadcast
0	192.168.1.0/26	192.168.1.1 - 192.168.1.62	192.168.1.63
1	192.168.1.64/26	192.168.1.65 - 192.168.1.126	192.168.1.127
2	192.168.1.128/26	192.168.1.129 - 192.168.1.190	192.168.1.191
3	192.168.1.192/26	192.168.1.193 - 192.168.1.254	192.168.1.255

Ejemplo con 6 subredes

Considera este ejemplo con cinco LAN y una WAN para un total de 6 redes.
Observa la figura.



Para incluir 6 redes, coloca la subred 192.168.1.0 /24 en bloques de direcciones mediante la fórmula: **$2^3 = 8$**
Para obtener al menos 6 subredes, pide prestados tres bits de host. Una máscara de subred **255.255.255.224 proporciona los tres bits de red adicionales.**

→ **Cantidad de hosts**

Para calcular la cantidad de hosts, comienza por examinar el último octeto. Observa estas subredes:

- 0 = **000**00000
- 32 = **001**00000
- 64 = **010**00000
- 96 = **011**00000
- 128 = **100**00000
- 160 = **101**00000
- 192 = **110**00000
- 224 = **111**00000

Aplica la fórmula de cálculo de host: **$2^5 - 2 = 30$ hosts por subred.**
Observa la figura del esquema de direccionamiento para estas redes.

Esquema de direccionamiento: Ejemplo de 6 redes

Subred	Dirección de red	Rango de host	Dirección de broadcast
0	192.168.1.0/27	192.168.1.1 – 192.168.1.30	192.168.1.31
1	192.168.1.32/27	192.168.1.33 – 192.168.1.62	192.168.1.63
2	192.168.1.64/27	192.168.1.65 – 192.168.1.94	192.168.1.95
3	192.168.1.96/27	192.168.1.97 – 192.168.1.126	192.168.1.127
4	192.168.1.128/27	192.168.1.129 – 192.168.1.158	192.168.1.159
5	192.168.1.160/27	192.168.1.161 – 192.168.1.190	192.168.1.191
6	192.168.1.192/27	192.168.1.193 – 192.168.1.222	192.168.1.223
7	192.168.1.224/27	192.168.1.225 – 192.168.1.254	192.168.1.255

12. ENRUTAMIENTO IP

El enrutamiento IP se refiere al proceso de llevar, un datagrama desde un ordenador origen a un ordenador destino sin importar que ambos pertenezcan a la misma red o no.

El enrutamiento se lleva a cabo gracias a un dispositivo de nivel de red ya estudiado, el router.

El router o encaminador mantiene las denominadas **tablas de enrutamiento** mediante las cuales conoce todas las redes que están conectadas a él.

Cuando un PC quiere enviar información lo primero que se pregunta la NIC es si el PC destino está en la misma red que él o no.

En caso de que no esté en la misma red el paquete será enviado al router (puerta de enlace) que se encargará de retransmitirlo al resto de redes.

Si el ordenador destino está en la misma red que el PC origen será el switch quien entre en juego. El switch asocia direcciones MAC con direcciones IP de forma que cuando debe enviar un datagrama con una IP destino dada, lo primero que hará será resolver la dirección MAC asociada a esta IP. Si es la primera vez que se envía un paquete con una dirección IP destino concreta, el switch debe averiguar la dirección MAC de ésta. El dispositivo enviará un paquete a toda la red (un broadcast) preguntando a quién pertenece la dirección IP destino (ARP Request). Solo el ordenador con IP igual a la preguntada responderá al broadcast. Cada switch mantiene una tabla en la que asocia dirección MAC de cada puerto y dirección MAC de cada NIC conectada a él.

TABLAS DE ENRUTAMIENTO

Las tablas de enrutamiento mantienen la información necesaria para que un datagrama pueda alcanzar cualquier destino más allá de la red en la que se ubica y están implementadas tanto en los routers como en los hosts. Normalmente, estará compuesta de los siguientes campos:

1. **Destino (D). IP de una red o host.** En destino podemos encontrar:
   - → **Ruta de red.** La entrada de la tabla hace referencia a toda una red.
   - → **Ruta de host.** La entrada de la tabla hace referencia a un host
   - → **Ruta por defecto (0.0.0.0).** Cuando ninguna de las entradas de la tabla resuelven el lugar donde se encuentra el equipo con IP destino, se usa la ruta por defecto. La ruta por defecto hará accesibles redes no contempladas directamente y delegará la búsqueda del host a otros encaminadores.
2. **Máscara de red (MR). Será la máscara de red correspondiente a Destino.**
3. **Puerta de enlace.** Dirección IP de la interfaz por la que accedo a D.
4. **Interfaz.** Corresponde con la puerta de enlace. En realidad, es el puerto en el router que conecta con el switch de la red.

Tabla de enrutamiento del router. Comando route print.

```
IPv4 Tabla de enrutamiento
===========================================================================
Rutas activas:
Destino de red        Máscara de red   Puerta de enlace   Interfaz  Métrica
          0.0.0.0          0.0.0.0  192.168.100.254  192.168.100.108    281
         10.2.8.0    255.255.255.0      En vínculo       10.2.8.100    281
       10.2.8.100  255.255.255.255      En vínculo       10.2.8.100    281
       10.2.8.255  255.255.255.255      En vínculo       10.2.8.100    281
        127.0.0.0        255.0.0.0      En vínculo        127.0.0.1    331
        127.0.0.1  255.255.255.255      En vínculo        127.0.0.1    331
  127.255.255.255  255.255.255.255      En vínculo        127.0.0.1    331
     192.168.44.0    255.255.255.0      En vínculo      192.168.44.1    291
```

```
C:\Users\Administrador>arp -a

Interfaz: 192.168.0.10 --- 0x1c
  Dirección de Internet          Dirección física      Tipo
  192.168.0.1           00-22-3a-e0-75-d8     dinámico
  192.168.0.11          00-0c-6e-d6-19-d4     dinámico
  192.168.0.13          00-1d-e0-05-1f-d7     dinámico
  192.168.0.255         ff-ff-ff-ff-ff-ff     estático
  224.0.0.22            01-00-5e-00-00-16     estático
  224.0.0.252           01-00-5e-00-00-fc     estático
  224.0.0.253           01-00-5e-00-00-fd     estático
  239.255.255.250       01-00-5e-7f-ff-fa     estático
```

13. CAPA DE TRANSPORTE

TCP y UDP

Los dos protocolos más comunes de la capa de transporte del conjunto de protocolos TCP/IP son el **Protocolo de control de transmisión (TCP)** y el **Protocolo de datagramas de usuario (UDP)**. Ambos protocolos gestionan la comunicación de múltiples aplicaciones. Las diferencias entre ellos son las funciones específicas que cada uno implementa.

Protocolo de datagramas de usuario (UDP)

UDP es un protocolo simple, sin conexión, descrito en la RFC 768. Cuenta con la ventaja de proveer la entrega de datos sin utilizar muchos recursos. Las porciones de comunicación en UDP se llaman datagramas. Este protocolo de la capa de transporte envía estos datagramas como "mejor intento".

Las aplicaciones que utilizan UDP incluyen:

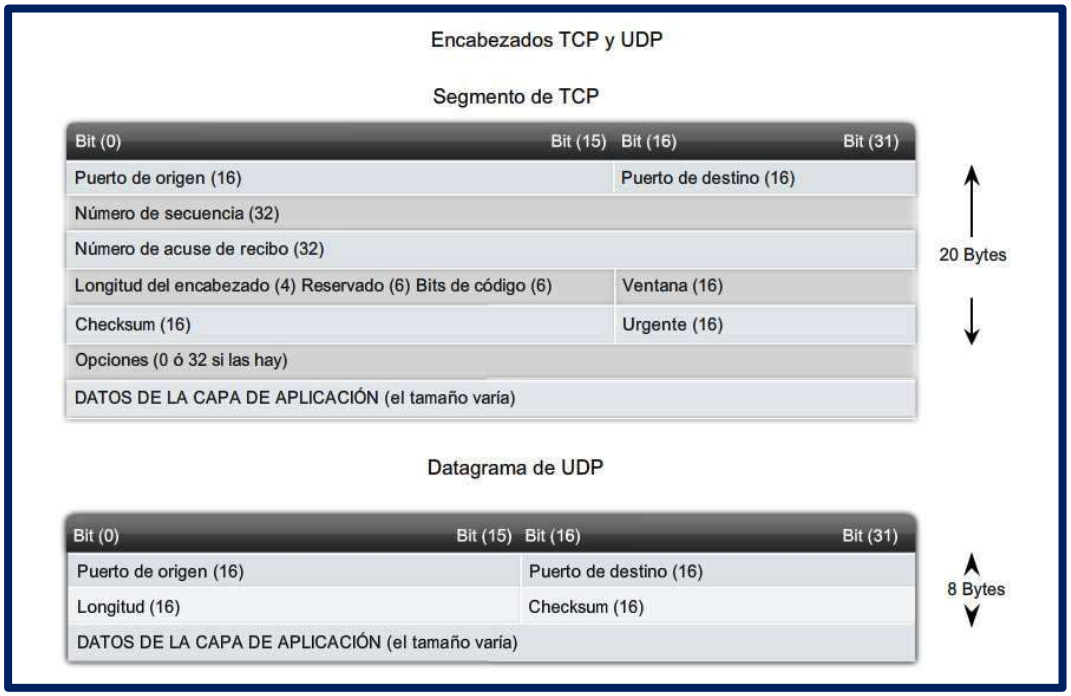
- → Sistema de nombres de dominio (DNS)
- → Streaming video
- → Voz sobre IP (VOIP)

Protocolo de control de transmisión (TCP)

TCP es un protocolo orientado a la conexión descrito en RFC 793. El TCP utiliza recursos adicionales para ganar funciones. Las funciones adicionales especificadas por TCP están en el mismo orden de entrega, son de entrega confiable y de control de flujo. Cada segmento de TCP posee 20 bytes de carga en el encabezado que encapsulan los datos de la capa de aplicación, mientras que cada datagrama UDP sólo posee 8 bytes de carga. Vea la figura para hacer una comparación.

Las aplicaciones que utiliza el TCP son:

- → Exploradores Web
- → Correo electrónico
- → Transferencias de archivos



Direccionamiento del puerto

Identificación de conversaciones

Consideremos el ejemplo de un ordenador que recibe y envía correos electrónicos, mensajes instantáneos, páginas web y llamadas telefónicas VoIP de manera simultánea.

Los servicios basados en TCP y UDP mantienen un seguimiento de las diversas aplicaciones que se comunican. Para diferenciar los segmentos y datagramas para cada aplicación, tanto TCP como UDP cuentan con campos de encabezado que pueden identificar de manera exclusiva estas aplicaciones. Estos identificadores únicos son números de puertos.

En el encabezado de cada segmento o datagrama, hay un puerto origen y uno de destino.

El número de puerto de origen es el número para esta comunicación asociado con la aplicación que origina la comunicación en el host local.

El número de puerto de destino es el número para esta comunicación asociado con la aplicación de destino que origina la comunicación en el host local.

Los números de puerto se asignan de distintas maneras, en virtud de si el mensaje es una solicitud o una respuesta. Mientras que los procesos del servidor tienen números de puerto estáticos asignados, los clientes eligen de forma dinámica un número de puerto para cada conversación.

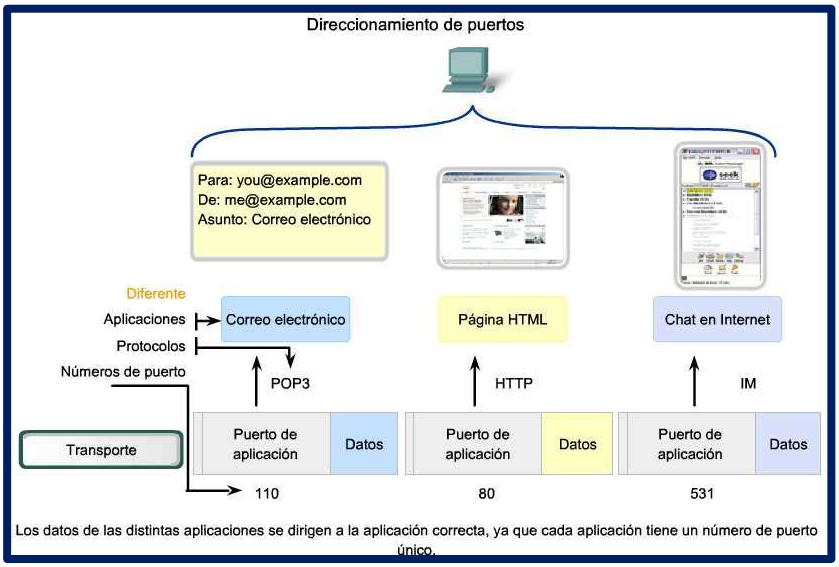
Cuando una aplicación de cliente envía una solicitud a una aplicación de servidor, el puerto de destino contenido en el encabezado es el número de puerto asignado al demonio de servicio que se ejecuta en el host remoto. El software del cliente debe conocer el número de puerto asociado con el proceso del servidor en el host remoto. Este número de puerto de destino se puede configurar, ya sea de forma predeterminada o manual. Por ejemplo, cuando una aplicación de explorador web realiza una solicitud a un servidor web, el explorador utiliza TCP y el número de puerto 80 a menos que se especifique otro valor. Esto sucede porque el puerto TCP 80 es el puerto predeterminado asignado a aplicaciones de servidores web. Muchas aplicaciones comunes tienen asignados puertos predeterminados.

El puerto de origen en el encabezado de un segmento o de un datagrama de la solicitud de un cliente se crea de forma aleatoria desde los números de puerto mayores de 1023. Mientras no haya un conflicto con otros puertos en uso en el sistema, el cliente puede elegir cualquier número de puerto del rango de números predeterminados que utiliza el sistema operativo. El número de puerto actúa como dirección de retorno para la aplicación que realiza la solicitud. La capa de transporte mantiene un seguimiento de este puerto y de la aplicación que generó la solicitud, de manera que cuando se devuelva una respuesta, se pueda ser enviar a la aplicación correcta. El número de puerto de la aplicación que realiza la solicitud se utiliza como número de puerto de destino en la respuesta que vuelve del servidor.

La combinación del número de puerto de la capa de transporte y de la dirección IP de la capa de red asignada al host identifica de manera exclusiva un proceso en particular que se ejecuta en un dispositivo host específico. Esta combinación se denomina socket. Eventualmente, los términos número de puerto y socket se utilizan en forma indistinta. En el contexto de este tema, el término socket hace referencia sólo a la combinación exclusiva de dirección IP y número de puerto. Un par de sockets, que consiste en las direcciones IP de origen y destino y los números de puertos, también es exclusivo e identifica la conversación entre los dos hosts.

Por ejemplo, una solicitud de página web HTTP que se envía a un servidor web (puerto 80) que se ejecuta en un host con una dirección IPv4 de Capa 3 de 192.168.1.20 se destinaría al socket 192.168.1.20:80.

Si el explorador web que solicita una página web se ejecuta en el host 192.168.100.48 y el número de puerto dinámico que se asignó al explorador es 49152, el socket para la página web sería 192.168.100.48:49152.



La Autoridad de números asignados de Internet (IANA) asigna números de puerto. IANA es un organismo normativo responsable de asegurar diferentes estándares de direccionamiento.
Hay diversos tipos de números de puerto:
Puertos bien conocidos (números del 0 al 1023): estos números se reservan para servicios y aplicaciones. Por lo general, se utilizan para aplicaciones como HTTP (servidor web), POP3/SMTP (servidor de correo electrónico) y Telnet. Al definir estos puertos bien conocidos para las aplicaciones de los servidores, las aplicaciones cliente se pueden programar para solicitar una conexión a dicho puerto y su servicio asociado.
Puertos registrados (números del 1024 al 49151): estos números de puerto se asignan a procesos o aplicaciones del usuario. Estos procesos son principalmente aplicaciones individuales que el usuario elige instalar en lugar de aplicaciones comunes que recibiría un puerto bien conocido. Cuando no se utilizan para un recurso del servidor, estos puertos se pueden utilizar también seleccionados de forma dinámica por un cliente como su puerto de origen.
Puertos dinámicos o privados (números del 49152 al 65535): también conocidos como puertos efímeros, están usualmente asignados de forma dinámica a las aplicaciones cliente cuando se inicia una conexión. No es muy común que un cliente se conecte a un servicio utilizando un puerto dinámico o privado (aunque algunos programas que comparten archivos punto a punto lo hacen).
Uso de TCP y UDP
Algunas aplicaciones pueden utilizar ambos. Por ejemplo, el bajo gasto de UDP permite que DNS atienda rápidamente varias solicitudes de clientes. Sin embargo, a veces el envío de la información solicitada puede requerir la confiabilidad de TCP. En este caso, el número de puerto bien conocido 53 lo utilizan ambos protocolos con este servicio.