

# Introducción a los Sistemas en Red.



# Índice

1.- Características de las redes de ordenadores.

    1.1.- Sistema de Comunicación.

    1.2.- Redes de ordenadores. Características.

    1.3.- Redes de ordenadores. Clasificación.

    1.4.- Redes de ordenadores. Ventajas.

    1.5.- Redes de ordenadores. Técnicas de Conmutación.

2.- La arquitectura de red.

    2.1.- Funcionamiento de una arquitectura basada en niveles.

    2.2.- Protocolo de comunicación.

    2.3.- Modelo OSI.

    2.4.- TCP/IP.

        2.4.1- El nivel de acceso a la red.

        2.4.2- El nivel de internet o de red.

        2.4.3- El nivel de transporte.

        2.4.4- El nivel de aplicación.

            2.4.4.1.- Servicios de Red

                - Servicio Web

                - Servicio Correo

                - Servicio DNS

                - Servicio DHCP

                - Servicio FTP

                - Servicio de acceso remoto

Nos encontramos en un **momento decisivo** respecto del **uso de la tecnología** para extender y **potenciar** nuestra capacidad de **comunicarnos**.

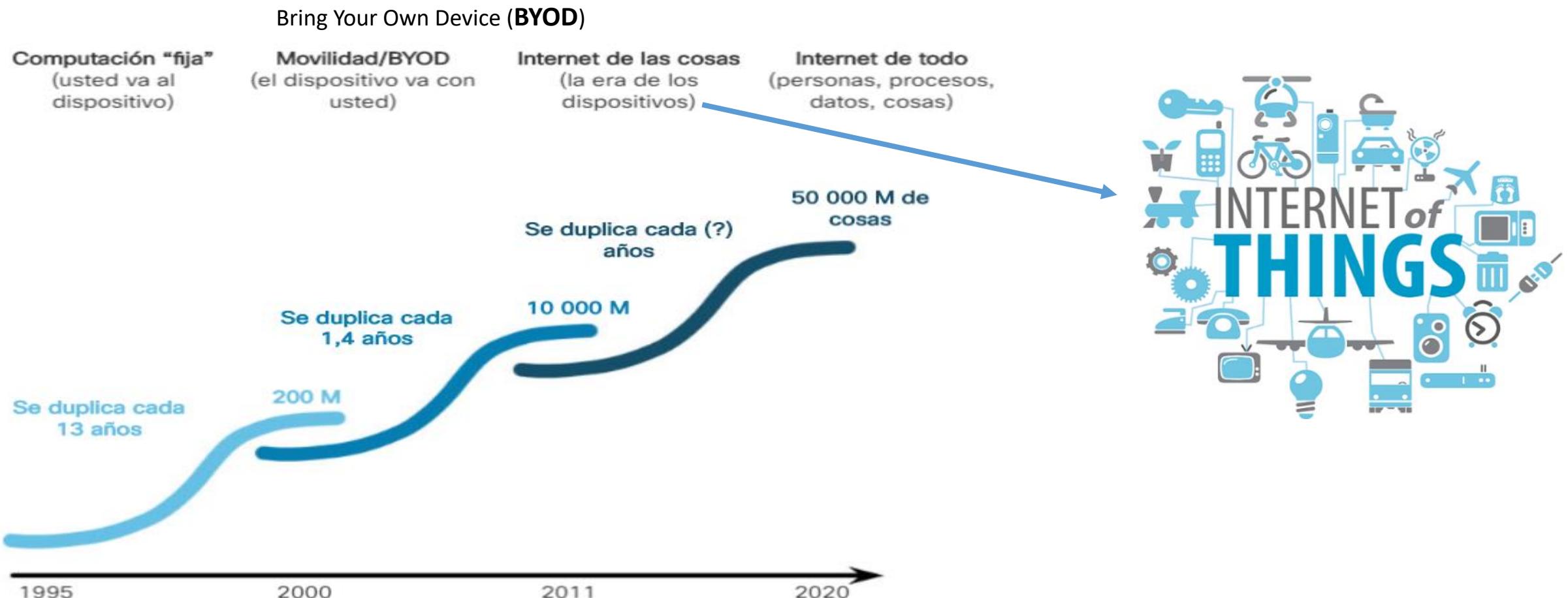
La **globalización** de Internet se ha producido **más rápido de lo que cualquiera hubiera imaginado**. El modo en que se producen las **interacciones sociales, comerciales, políticas y personales cambia en forma continua** para estar al día con la evolución de esta red global.

Internet se usará **como punto de inicio para esfuerzos innovadores**, lo que generará **nuevos productos y servicios** diseñados específicamente para aprovechar las capacidades de la red. A medida que los **programadores impulsen los límites de lo posible**, las **capacidades de las redes interconectadas** que crean Internet jugarán un **papel cada vez más grande** en el éxito de estos proyectos.



Estamos **conectados** como nunca antes gracias al uso de redes:

- Las personas que tienen alguna idea pueden **comunicarse de manera instantánea con otras personas para hacer esas ideas realidad.**
- Las **noticias y los descubrimientos se conocen en todo el mundo en cuestión de segundos.**
- Incluso, las personas pueden **conectarse y jugar con amigos en otros continentes.**



- Para el año 2014, el tráfico de los dispositivos inalámbricos excederá el tráfico de los dispositivos conectados por cable.
- Para el año 2015, la cantidad de contenido que fluya anualmente por Internet será 540 000 veces la cantidad que se transmitió en 2003.
- Para el año 2015, el 90% de todo el contenido en Internet estará basado en video.
- Para el año 2015, un millón de minutos de video atravesarán Internet por segundo.
- Para el año 2016, el tráfico IP global anual superará el umbral del zettabyte (1 180 591 620 717 411 303 424 bytes).
- Para el año 2016, la cantidad de dispositivos conectados a redes IP será aproximadamente tres veces la población mundial.
- Para el año 2016, 1,2 millones de minutos de contenido de video atravesarán la red por segundo.
- Para el año 2020, habrá 50 000 millones de dispositivos conectados a Internet.

El concepto de **internet de todo** se originó en Cisco, define IoE como "la **conexión inteligente de personas, procesos, datos y cosas**".

En la internet de las cosas, todas las comunicaciones **son entre máquinas, IoT y M2M** a veces son considerados sinónimos. El concepto IoE es más **expansivo** incluye, además de las comunicaciones M2M, las **interacciones de máquina a persona (M2P)** y las de **persona a persona (P2P)** asistida por tecnología.



Una pequeña introducción sobre IoE (Internet OF Everything):

<https://searchdatacenter.techtarget.com/es/definicion/Internet-de-todo-IoE>

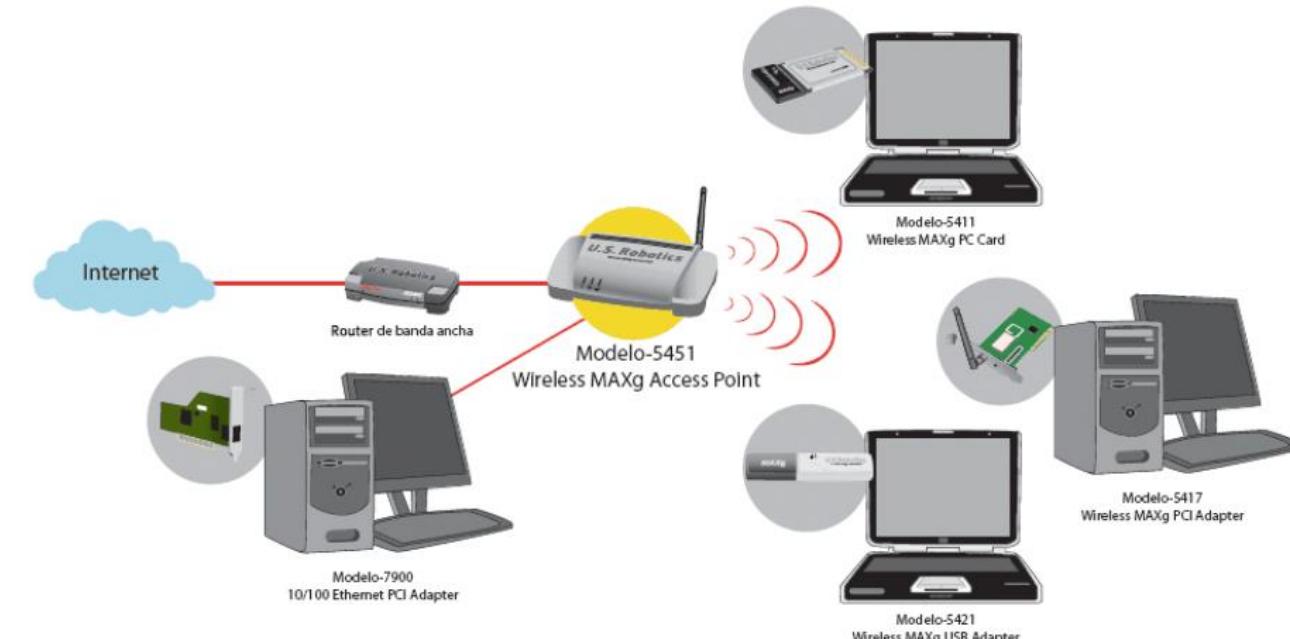
En la actualidad más del 99% del mundo está desconectado, mañana conectaremos todo.

<https://www.youtube.com/watch?v=D2AZIM8KdN8>



Para ampliar tus conocimientos, y como referencia para los demás puntos a desarrollar en la unidad, te sugerimos que consultes el artículo de la Wikipedia relacionado con las redes de computadoras, te ayudará a estudiar los siguientes apartados.

[http://es.wikipedia.org/wiki/Red\\_de\\_computadoras](http://es.wikipedia.org/wiki/Red_de_computadoras)



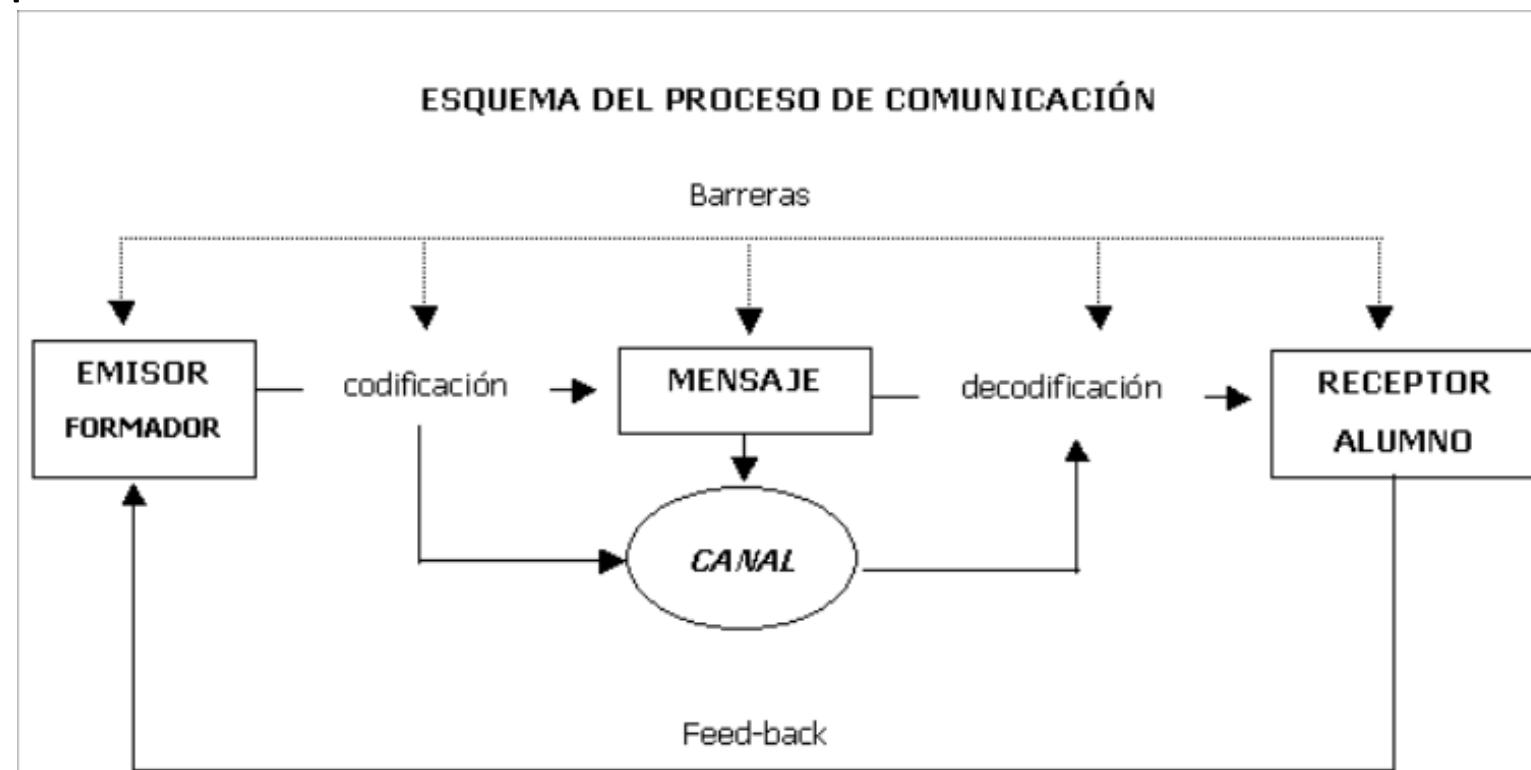
## Sistema de comunicación.

- **Sistema:** es el **conjunto de reglas o principios** sobre una materia **racionalmente enlazados entre sí**.
- **Comunicación:** se puede definir como **transmisión de señales mediante un código común al emisor y al receptor**.
- **Sistema de comunicación:** como un **conjunto de elementos que, siguiendo unas reglas, intervienen en la transmisión de señales**, permitiendo el intercambio de información entre un emisor y un receptor.

De esta definición podemos inferir los **componentes de un sistema de comunicación**, que serán:

- **Emisor:** elemento que transmite la información.
- **Receptor:** elemento que recibe la información.
- **Canal:** medio por el cual se transmite la información, utilizando señales convenientemente codificadas.

- **Protocolo de comunicación:** es necesario que emisor y receptor **codifiquen la información de forma que ambos se entiendan**, por tanto necesitan crear un **conjunto de reglas que regulen la comunicación entre ambos**, este conjunto de reglas es lo que conocemos por protocolo de comunicación.
- **Canal de comunicaciones:** considerando que la **transferencia de la información** entre emisor y receptor se lleva a cabo a través del canal de comunicaciones, podemos definir este último como el **medio físico por el cual se transporta la información convenientemente codificada**, siguiendo unos protocolos establecidos.

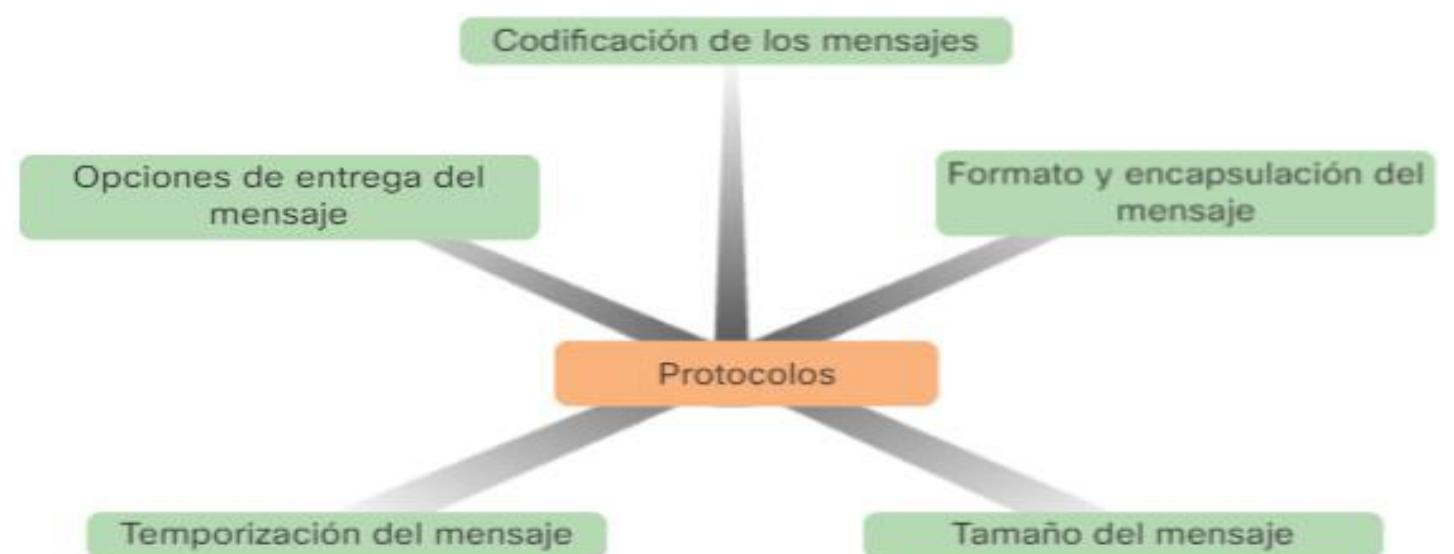


Antes de comunicarse entre sí, las personas deben **utilizar reglas o acuerdos** establecidos que ríjan la conversación.

Estas reglas, o **protocolos**, deben **respetarse** para que el mensaje se envíe y comprenda correctamente. Se encuentran disponibles muchos protocolos que rigen la **comunicación humana correcta**. Una vez que se acuerda un método de comunicación (cara a cara, teléfono, carta, fotografía), los protocolos implementados deben contemplar los siguientes **requisitos**:

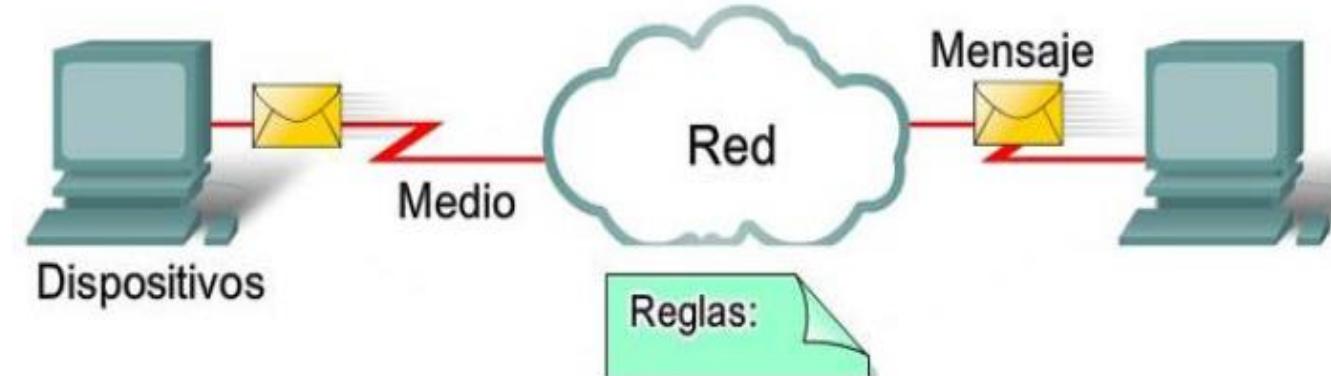
- Un **emisor** y un **receptor** identificados
- **Idioma** y gramática común
- Velocidad y **temporización** de la entrega
- Requisitos de confirmación o **acuse de recibo**

Los protocolos que se utilizan en las **comunicaciones de red** comparten muchas de las características fundamentales



Actividad. En los siguientes ejemplos distingue entre emisor, receptor y canal:

- Una noticia en la radio.
- Dos amigos hablando en la calle.
- Un ordenador descargando un archivo de Internet.



Actividad: identificar posibles barreras que podemos encontrar en el proceso de comunicación:

- Físicas: Distancia, Ruido, Iluminación, Medios
- Fisiológicas: en emisor o receptor
- Lenguaje
- Burocráticas
- Semánticas: mismas palabras con diferentes significados
- Sobrecarga de Información



Las redes están en todas partes, y las **redes de ordenadores** forman parte de ese **sistema de conexión global** cada vez más extendido, conocido como **Internet**.

Como futuro profesional del sector de la informática, una de las cosas que debes conocer es:

- **cómo trabajan los ordenadores** trabajan y **cómo se conectan entre sí para formar sistemas más amplios** que, en la mayoría de los casos, utilizan **redes de diferentes características**.

Definimos **red informática** como **dos o más dispositivos conectados para compartir**:

- **los componentes de su red**
- **la información** que pueda almacenarse en todos ellos.

Es decir, al menos dos ordenadores conectados entre sí mediante algún medio, que se **comunican y transmiten información**.

*Definición dada por Andrew S. Tanenbaum, una **red de computadoras**, también llamada **red de ordenadores** o **red informática**, es un **conjunto de equipos informáticos conectados entre sí por medio de dispositivos físicos que envían y reciben impulsos eléctricos, ondas electromagnéticas o cualquier otro medio para el transporte de datos**, con la finalidad de **compartir información y recursos**.*

Estos dos conceptos son parecidos en significado pero presentan diferencias:

- **Transmisión:** es el **transporte de la señal** donde viajan los datos . 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, solo **importan los datos que se están proporcionando** ambos elementos de la red.

*NOTA: No siempre que se transmite se está comunicar*

En definitiva para poder **trabajar con las redes de ordenadores** necesitamos conocer:

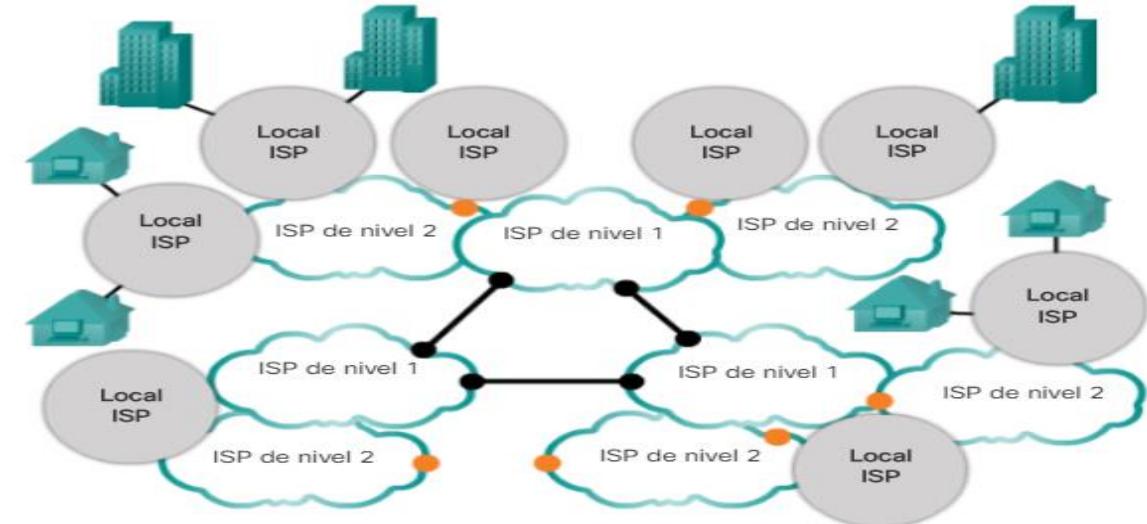
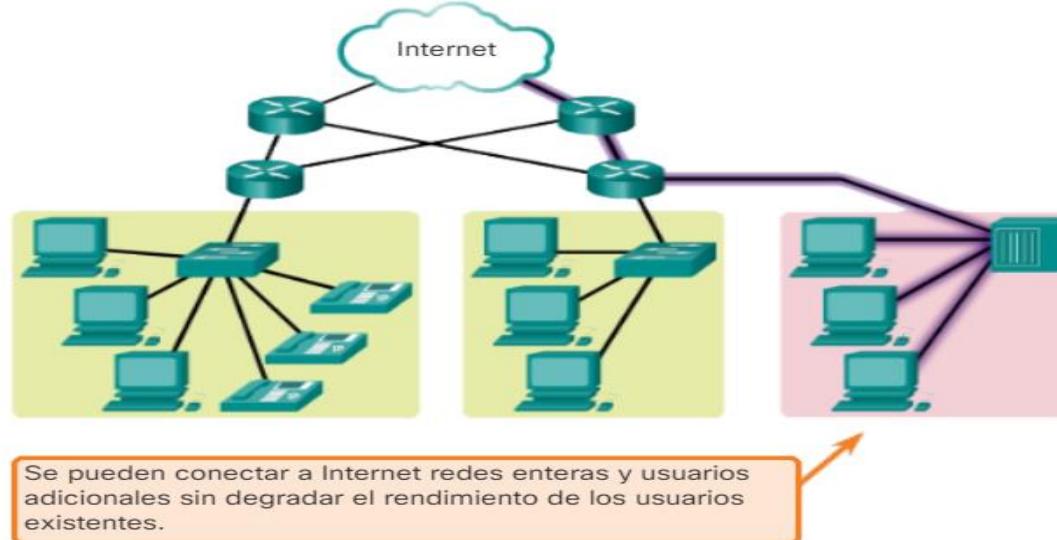
- los **sistemas de comunicación** más utilizados.
- la **arquitectura** que las hace posible.
- los **protocolos** asociados.
- la **forma de conectarlas y sus componentes**.



# Características de las Redes de Ordenadores:

Aunque en el desarrollo de la unidad veremos diferentes **características** de las redes de ordenadores, es conveniente empezar citando **algunas de las más importantes**, y que han contribuido a su generalización:

- **Conectividad:** La posibilidad de conexión de diferentes dispositivos entre sí con la finalidad de **compartir recursos** propios o ajenos, tanto en entornos **locales** como en entornos **remotos**.
- **Escalabilidad:** Una red de ordenadores puede **ampliar fácilmente sus posibilidades**, además esta red puede conectarse con otras redes, y así dar mayores prestaciones.



- **Seguridad:** Esta característica es **deseable y necesaria**, aunque no siempre se cuida lo suficiente. Es conveniente considerar esta característica como **una de las más importantes**. En algunos casos las redes:
  - **aumentan la seguridad ante pérdidas de datos**, ya que duplican información
  - en otros casos **disminuyen** la seguridad de esos datos, ya que están más disponibles.

The image shows a credit card statement from "Your First Bank". The statement is dated 3/13/01 and the payment due date is 3/09/01. The account number is 4125-235-412 and the name is John Doe. The credit line is \$1200.00 and the current balance is \$1074.76. The minimum payment due is \$20.00. The statement includes a table of transactions and a summary of previous purchases, cash advances, payments, credits, and finance charges.

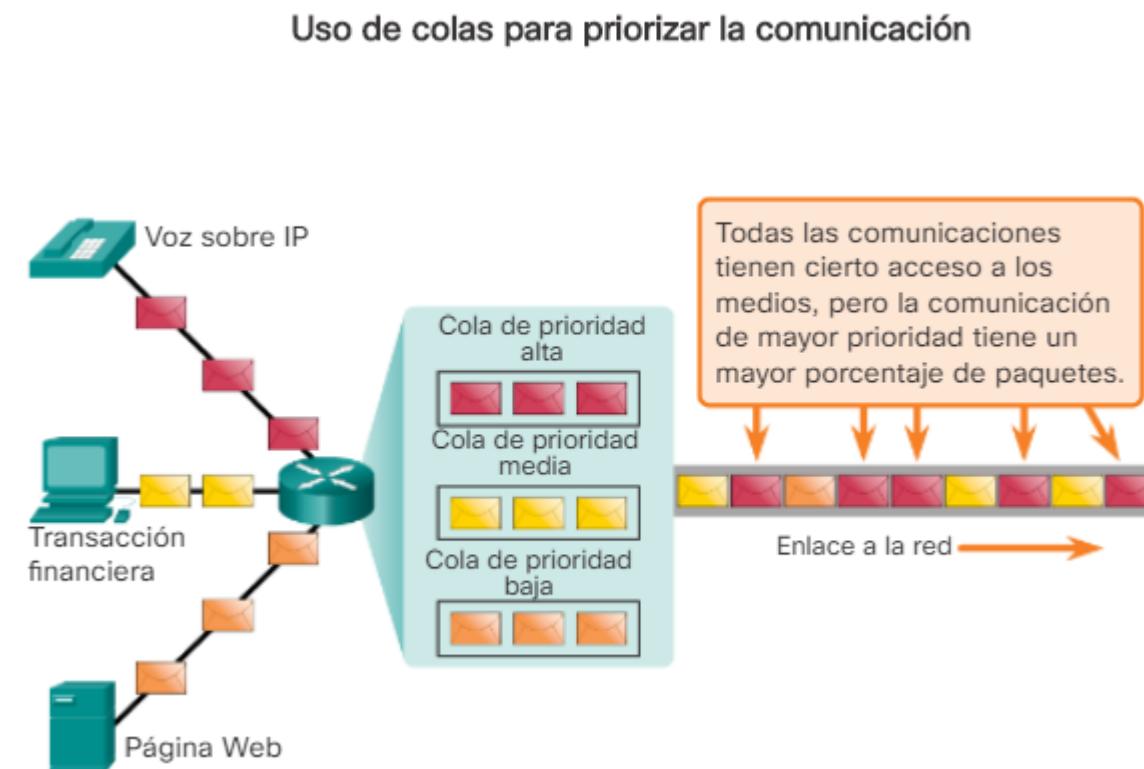
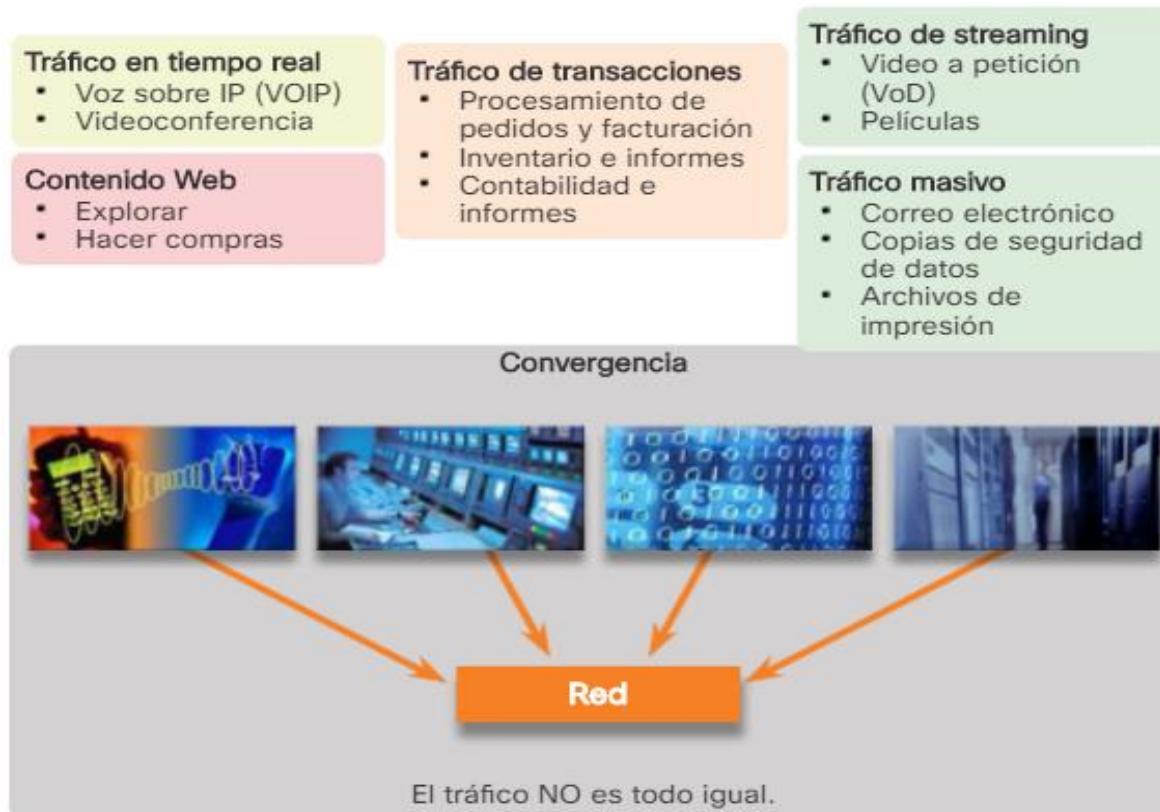
REFERENCE	SOLD	POSTED	ACTIVITY SINCE LAST STATEMENT	AMOUNT
483087382		3/25	PAYMENT THANK YOU	-100.00
327348883	1/12	3/15	RECORD RECYCLER	14.83
891020682	1/13	3/15	REPORAMA REST	30.55
5034928512	1/18	3/18	GREAT INSPECTORATIONS	21.50
04K77293A	1/20	3/21	JUNO-GUL PETROLEUM	17.24
87306321	2/09	3/09	SHREWS 'N SUCH	40.10

Previous Balance: (+) 100.00      Current Amount Due: 125.24  
Purchases: (+) 125.24      Amount Paid Due:  
Cash Advances: (-)      Amount Over Credit Line:  
Payments: (-) 100.00      Minimum Payment Due: 20.00  
Credits: (-)  
FINANCE CHARGES: (+)



- **Optimización de costes:** Si podemos **compartir recursos**, y estos recursos nos dan una **mayor productividad**, además de facilitarnos el trabajo, estamos optimizando costes y sacando mayor rendimiento a nuestra inversión.

- **Calidad de servicio (QoS):** Las redes deben proporcionar **servicios predecibles, mensurables y, en ocasiones, garantizados.** La arquitectura de red conmutada por paquetes no garantiza que todos los paquetes que conforman un mensaje en particular lleguen a tiempo y en el orden correcto, ni tampoco garantiza la llegada.



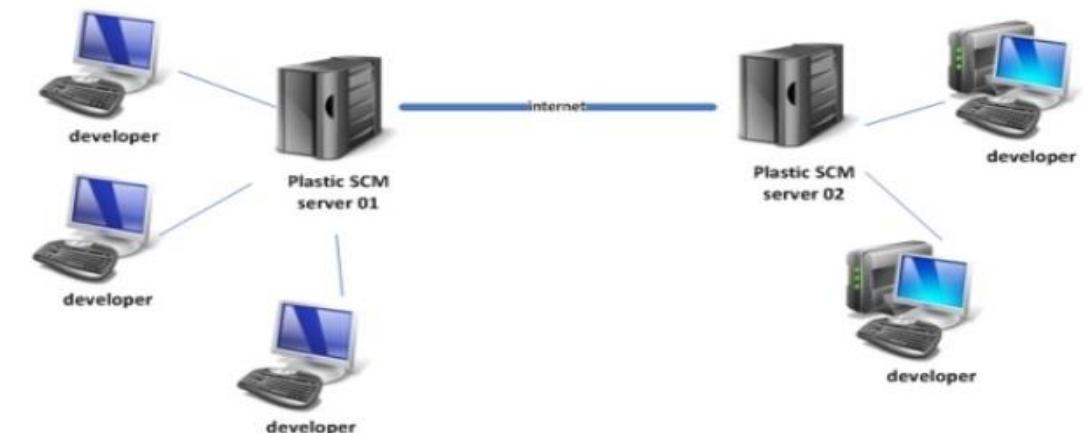
**El ancho de banda de la red** es la medida de la **cantidad de bits que se pueden transmitir en un segundo**, es decir, **bits por segundo (bps)**. Cuando se producen intentos de comunicaciones simultáneas a través de la red, la demanda de ancho de banda puede exceder su disponibilidad, lo que provoca congestión en la red.

# Clasificación de Redes.

Podemos realizar una primera clasificación atendiendo al **estado de aislamiento** o conexión de un sistema informático:

- **Sistemas aislados:** ordenadores que **no son capaces de conectarse, ni compartir información** con otro ordenador vía telemática.
- **Sistemas en red:** son los más usuales. Son **ordenadores conectados entre sí** gracias al uso de un **medio de conexión concreto**.
- **Sistemas distribuidos:** es similar a los sistemas en red. Su **peculiaridad es el lugar donde se encuentren los ordenadores**, etc., aunque esos datos son transparentes al usuario. Cada máquina posee sus componentes hardware y software, que el **usuario percibe como un solo sistema** (no necesita saber qué cosas están en qué máquinas). El usuario accede a los componentes de software/hardware remotos, de la **misma manera en que accedería a componentes locales**.

Se establece la comunicación mediante un protocolo prefijado por un **esquema “cliente-servidor”**.

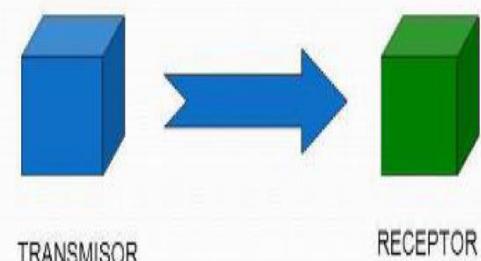


- Si el criterio que utilizamos es la **direccionalidad de la transmisión**, los sistemas de comunicación pueden clasificarse en:
  - **Simplex**: Cuando la comunicación se efectúa en un sólo sentido. Emisor emite, receptor recibe. **Ejemplo**: Cuando escuchamos música por la radio, nosotros sólo recibimos.
  - **Semidúplex (half duplex)**: Cuando la comunicación se realiza en los dos sentidos, pero no de forma simultánea. Emisor emite, receptor recibe, receptor pasa a ser emisor, y emisor pasa a ser receptor. **Ejemplo**: Hablar por el walkie-talkie.
  - **Dúplex (full duplex)**: Cuando la comunicación se realiza en ambos sentidos de forma simultánea. Ambos son emisores y receptores a la vez. **Ejemplo**: Las redes de ordenadores suelen funcionar de esta forma.

*Si quieres conocer más detalles relacionados con los conceptos de simplex, semidúplex y dúplex, te sugerimos que leas el siguiente artículo: [http://es.wikipedia.org/wiki/D%C3%BAplex\\_%28telecomunicaciones%29](http://es.wikipedia.org/wiki/D%C3%BAplex_%28telecomunicaciones%29)*

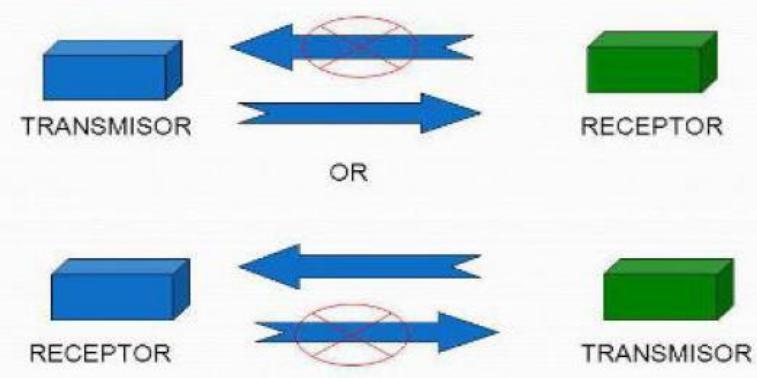
#### ➤ Comunicación Simplex

Sólo permiten la transmisión en un sentido



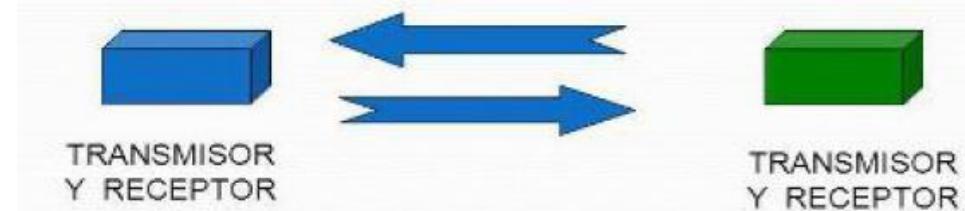
#### ➤ Comunicación Half Duplex

Sólo permiten la transmisión en los dos sentidos, pero no de forma simultánea



#### ➤ Comunicación Full Duplex

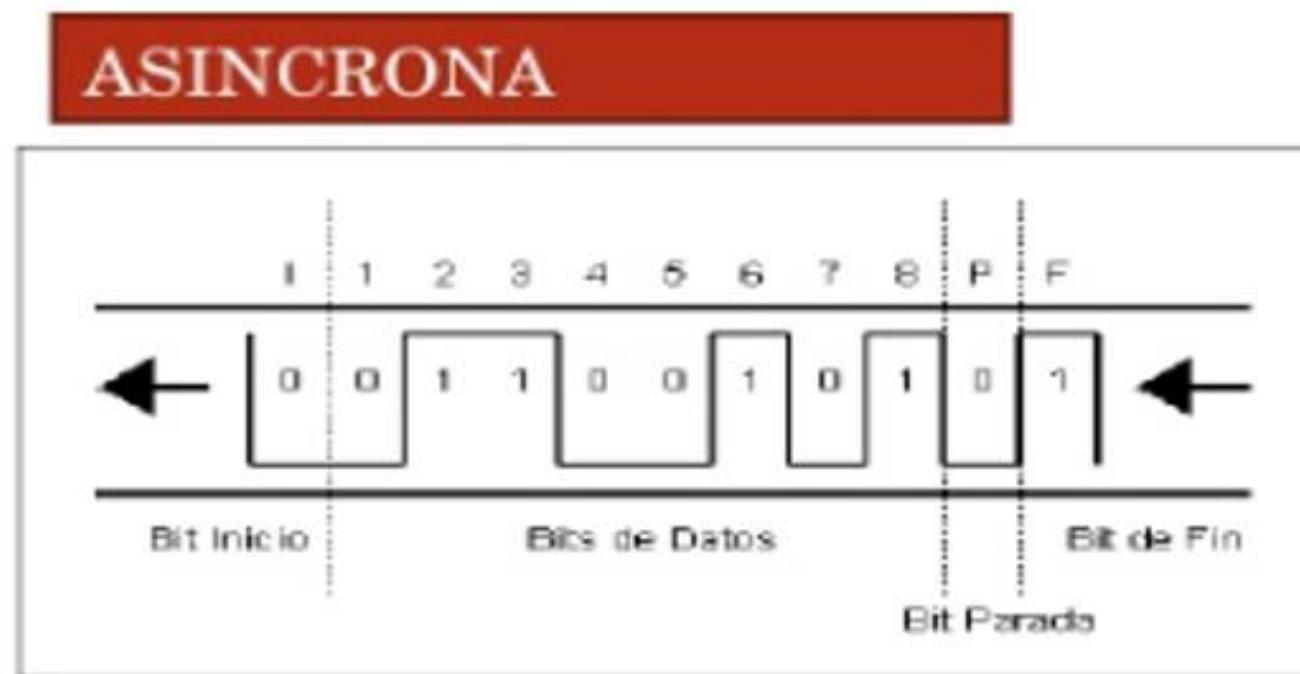
Permiten transmisión en los dos sentidos, en forma simultánea. La mayoría de los sistemas y redes de comunicaciones modernos funcionan en modo dúplex permitiendo canales de envío y recepción simultáneos



- Otros criterios que se utilizan para clasificar las comunicaciones es según la **forma de sincronizar** las señales, así tenemos comunicaciones:
  - **Asíncrona:**
    - el proceso de sincronización entre emisor y receptor se realiza en cada palabra de código transmitido. Esta sincronización se lleva a cabo a través de unos bits especiales que definen el entorno de cada código.
    - no hay ninguna relación temporal entre la estación que transmite y la que recibe. Es decir, el ritmo de presentación de la información al destino no tiene por qué coincidir con el ritmo de presentación de la información por la fuente. El receptor no sabe con precisión cuando recibirá un mensaje.
    - cada carácter a ser transmitido es delimitado por un bit de información denominado de cabecera o de arranque, y uno o dos bits denominados de terminación o de parada.
    - se suele agregar un bit de paridad (par o impar). Dicho Bit sirve para comprobar que los datos se transfieran sin interrupción.

## Ventajas y desventajas:

- En caso de errores se pierde siempre una cantidad pequeña de caracteres, pues éstos se sincronizan y se transmiten de uno en uno.
- Bajo rendimiento de transmisión, dada la proporción de bits útiles y de bits de sincronismo, que hay que transmitir por cada carácter.
- Es un procedimiento que permite el uso de equipamiento más económico y de tecnología menos sofisticada.
- Se adecua más fácilmente en aplicaciones, donde el flujo transmitido es más irregular.
- Son especialmente aptos, cuando no se necesitan lograr altas velocidades.



- **Síncrona:**

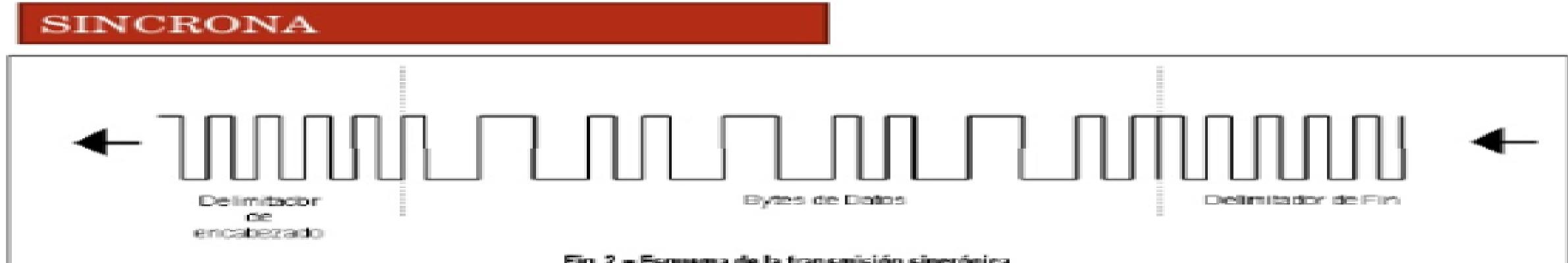
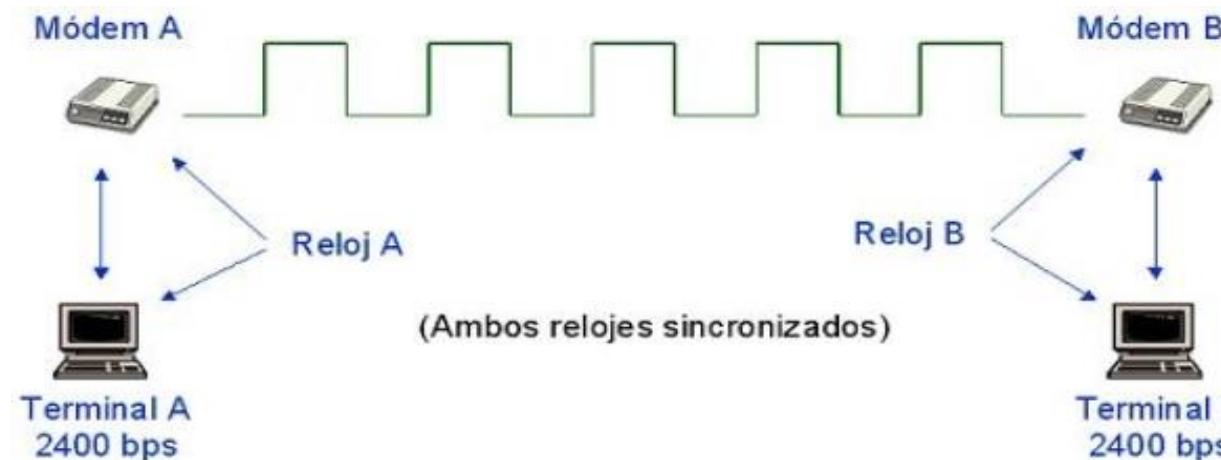
- técnica que consiste en el **enviar una trama** de datos (conjunto de caracteres) que configura un bloque de información **comenzando con un conjunto de bits de sincronismo (SYN)** y **terminando con otro conjunto de bits de final de bloque (ETB)**. En este caso, los bits de sincronismo tienen la función de **sincronizar los relojes existentes tanto en el emisor como en el receptor**, de tal forma que estos controlan la duración de cada bit y carácter.

## Ventajas:

- Posee un alto **rendimiento** en la transmisión
  - Aptos para transmisiones de **altas velocidades**
  - El flujo de datos es más **regular**

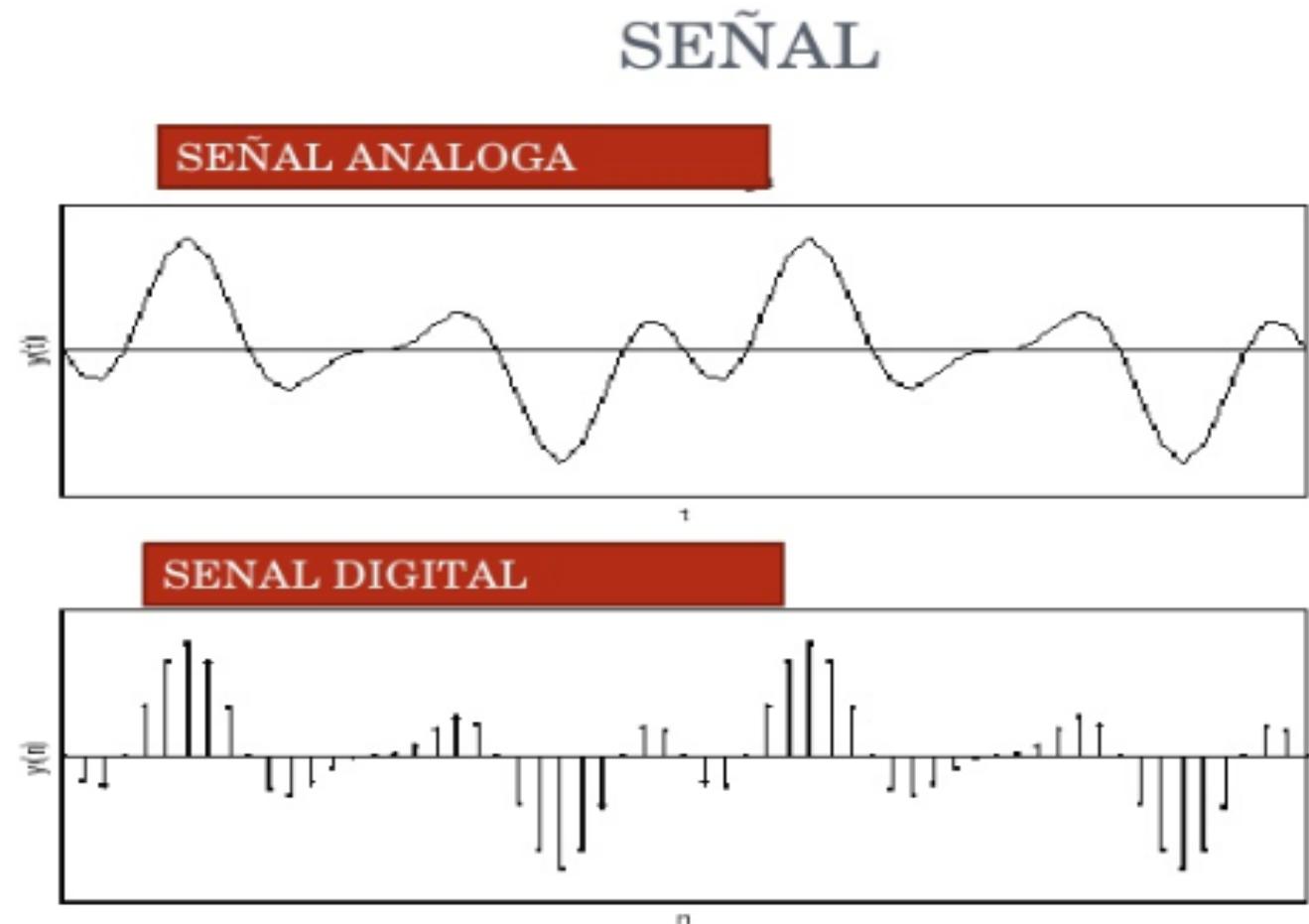
## **Desventaja:**

- Equipamientos de tecnología más completa y costos más altos



- Según la **naturaleza de la señal**, este criterio nos lleva a utilizar los términos de **trasmisiones** ( ya que los ordenadores son sistemas que se basan en el uso de señales digitales) / comunicaciones:
  - Analógicas.
  - Digitales.

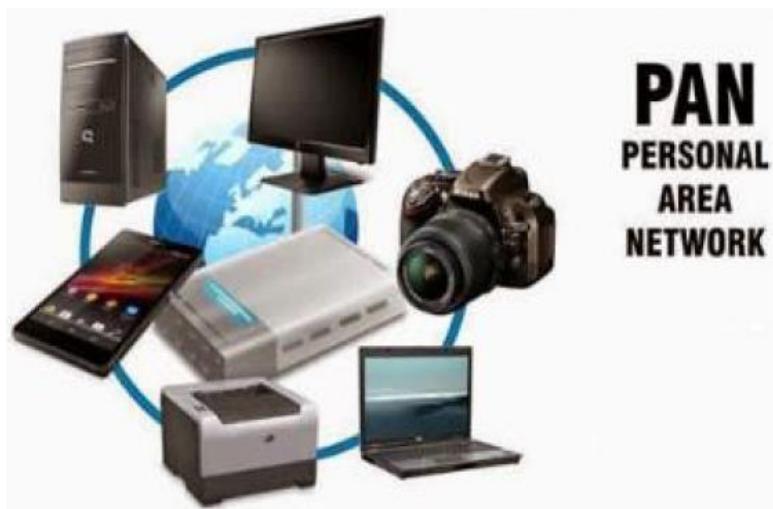
*La señal digital es un tipo de señal en que cada signo que codifica el contenido de la misma puede ser analizado en término de algunas **magnitudes que representan valores discretos**, en lugar de valores dentro de un cierto rango.*



# Clasificación de redes más utilizada.

Ya comentamos que las redes se pueden clasificar según diferentes conceptos, uno de los conceptos **más utilizados** es:

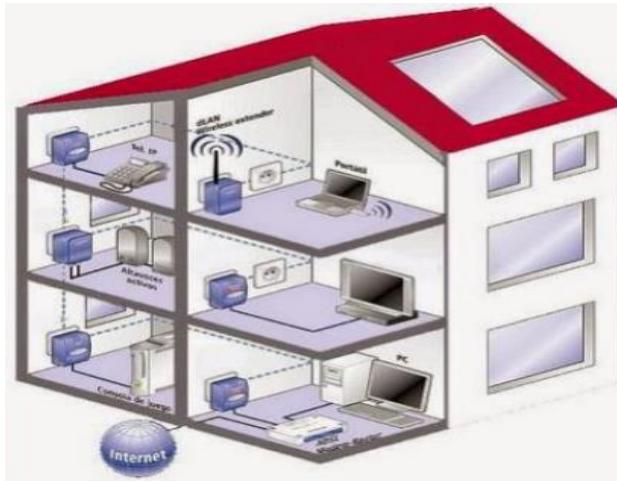
- Por alcance o **extensión** tenemos:
  - Red de **área personal** o **PAN** (personal area network): es una red de ordenadores usada para la **comunicación entre los dispositivos del ordenador cerca de una persona**.



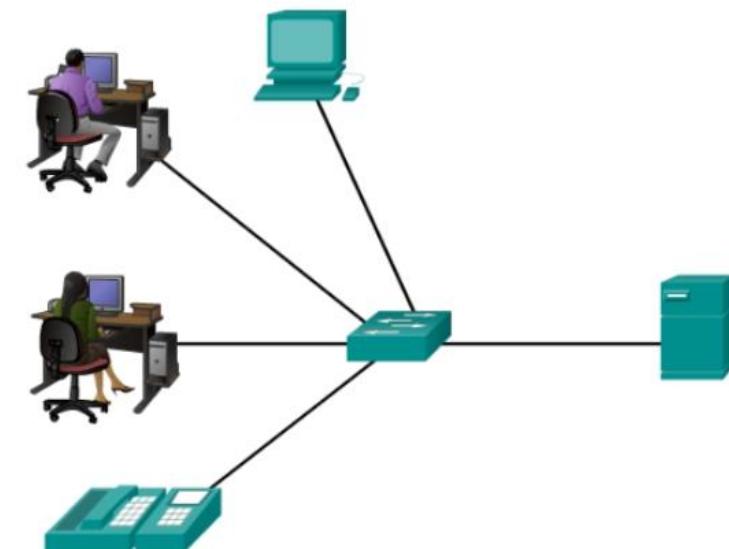
- Computadoras personales
- Impresoras
- Máquinas de fax
- Smartphone
- PDA
- Escáneres
- Consolas de videojuegos

- Red de área local o LAN (local area network):

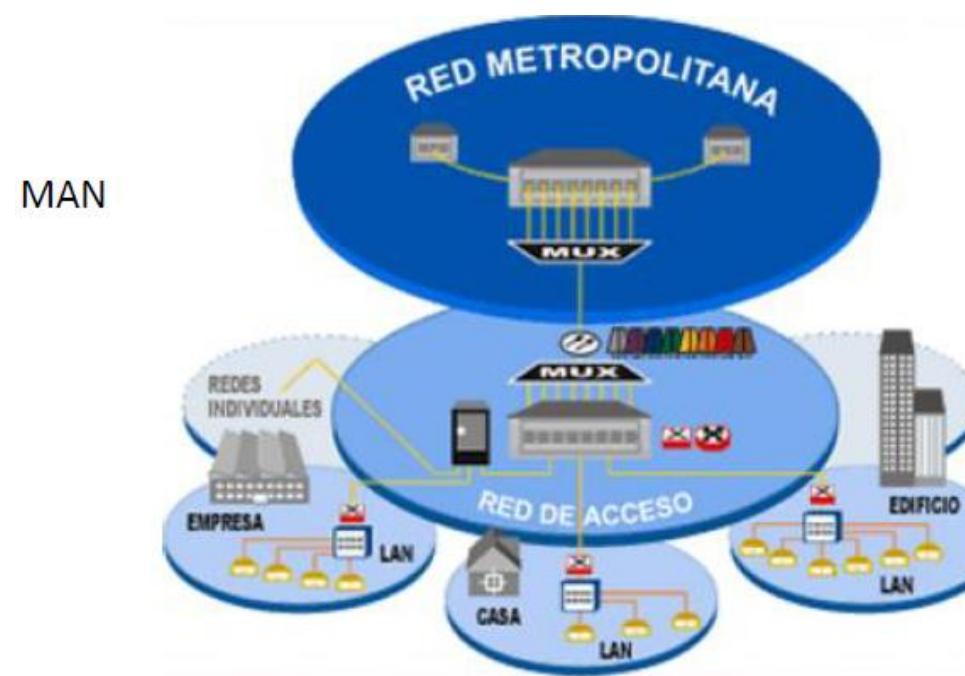
- Es una red que se **limita a un área especial, relativamente pequeña.**
- Las redes de área local suelen tener las **mayores velocidades**, además son el **componente esencial para la creación de redes más grandes.**
- Desprovistas de medios de interconexión públicos.
- Pueden servir a numerosos usuarios a la vez.
- La **administración** de las LAN está a cargo de **una única organización o persona**. El control administrativo que rige las políticas de seguridad y control de acceso está **implementado en el nivel de red.**



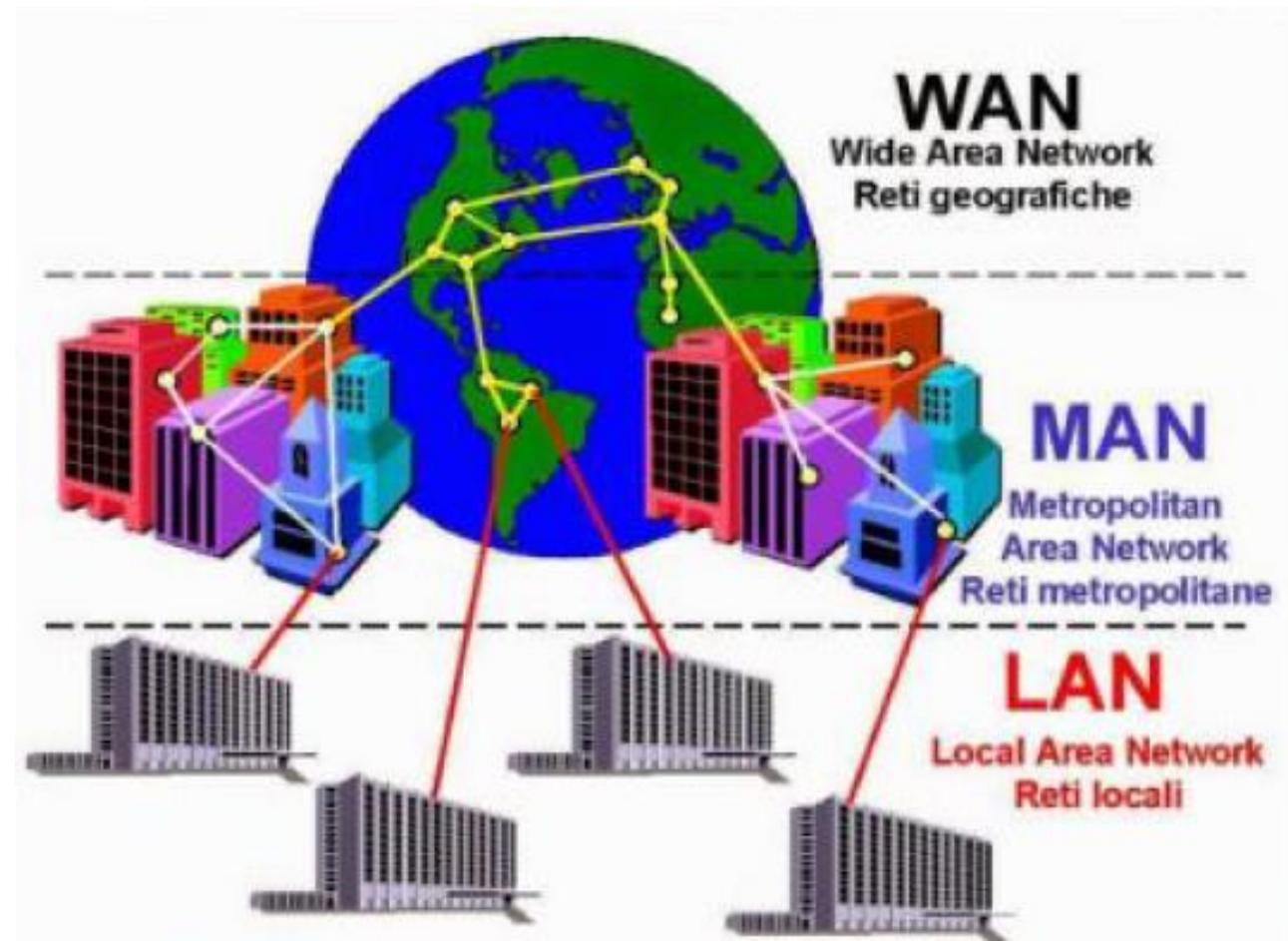
- Un cuarto
- Un aula
- Un solo edificio
- Una nave
- Un avión
- Un departamento



- Red de área de campus o **CAN** (campus area network) es una red de computadoras que **conecta redes de área local a través de un área geográfica limitada**, como un campus universitario, o una base militar. Este término se suele utilizar como **extensión del de LAN**, ya que realmente lo que se tiene son redes locales conectadas entre sí para abarcar una área más extensa.
- Red de área metropolitana o **MAN** (metropolitan area network) es una red de alta **velocidad** (banda ancha) que da **cobertura en un área geográfica más extensa que una LAN** (**de hecho contiene varias de ellas**), pero aun así **concreta y definida, como una porción de una ciudad**.



- Red de área amplia o WAN (wide area network) son redes informáticas que se extienden sobre un área geográfica extensa. Se trata de redes de amplio alcance y alta velocidad, que echan mano a satélites, cableados, microondas y nuevas tecnologías para cubrir una extensa porción geográfica. Dentro de esta clasificación podemos encontrar las redes de telecomunicaciones que permiten el uso de Internet, y el propio **Internet** que puede considerarse como una gigantesca red WAN.



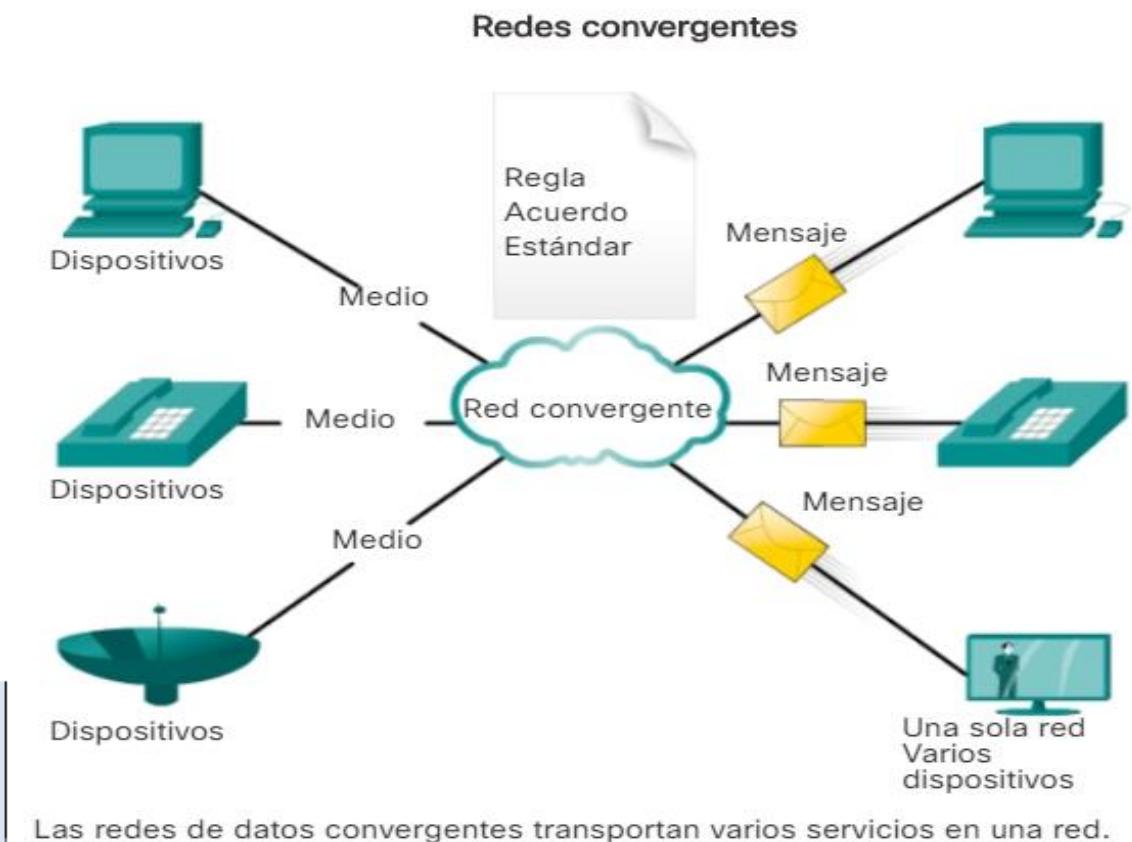
En el contexto de redes, “**convergencia**” es un término utilizado para describir el proceso por el cual se **combinan** comunicaciones de **voz, video y datos** en una **infraestructura de red común**.

Las redes convergentes existen hace tiempo, pero solo fueron viables a **grandes organizaciones empresariales** debido a los **requisitos de infraestructura de red** y a la **compleja administración** requerida para que funcionen sin inconvenientes.

Los avances tecnológicos pusieron la convergencia a **disposición** de las grandes, medianas y pequeñas empresas, así como del **consumidor doméstico**.

**Actividad** Indicar qué ISP locales en vuestra área ofrecen servicios convergentes para consumidores finales, utilizar el siguiente formulario predefinido.

Proveedor de servicios de Internet (Internet Service Provider)	Nombre de producto del servicio convergente	Costo por mes	Velocidad de descarga



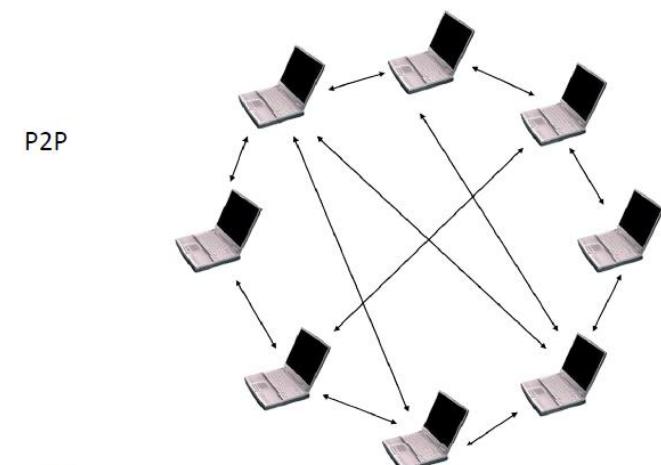
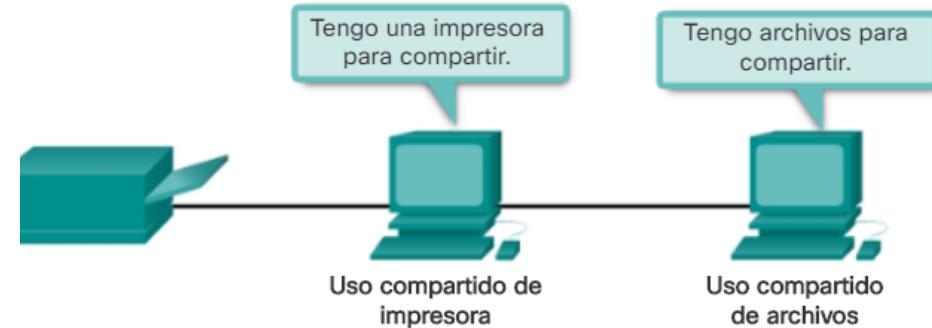
- **Según las funciones de sus componentes:**
  - Redes de **igual a igual o entre iguales**, también conocidas como redes **peer-to-peer**, son redes donde **ningún ordenador está a cargo del funcionamiento de la red**. Cada ordenador controla su propia información y puede funcionar como cliente o servidor según lo necesite. Los sistemas operativos más utilizados incluyen la posibilidad de trabajar de esta manera, y una de sus características más destacadas es que **cada usuario controla su propia seguridad**.

Ventajas de las redes punto a punto:

- Configuración sencilla.
- Menor complejidad.
- Bajo costo, dado que es posible que no se necesiten dispositivos de red ni servidores dedicados.
- Se pueden utilizar para tareas sencillas como transferir archivos y compartir impresoras.

Desventajas de las redes punto a punto:

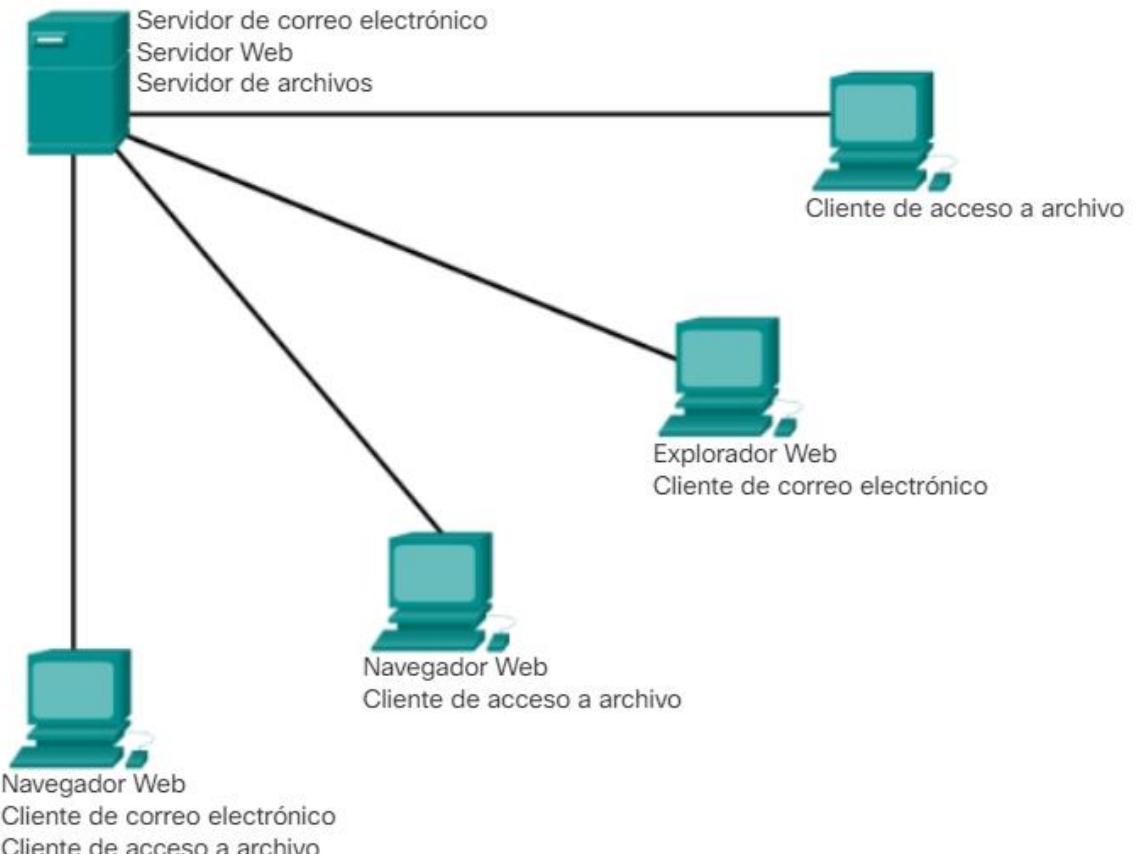
- La administración no está centralizada.
- No son tan seguras.
- No son escalables.
- Todos los dispositivos pueden funcionar como clientes y como servidores, lo que puede lenticular el funcionamiento.



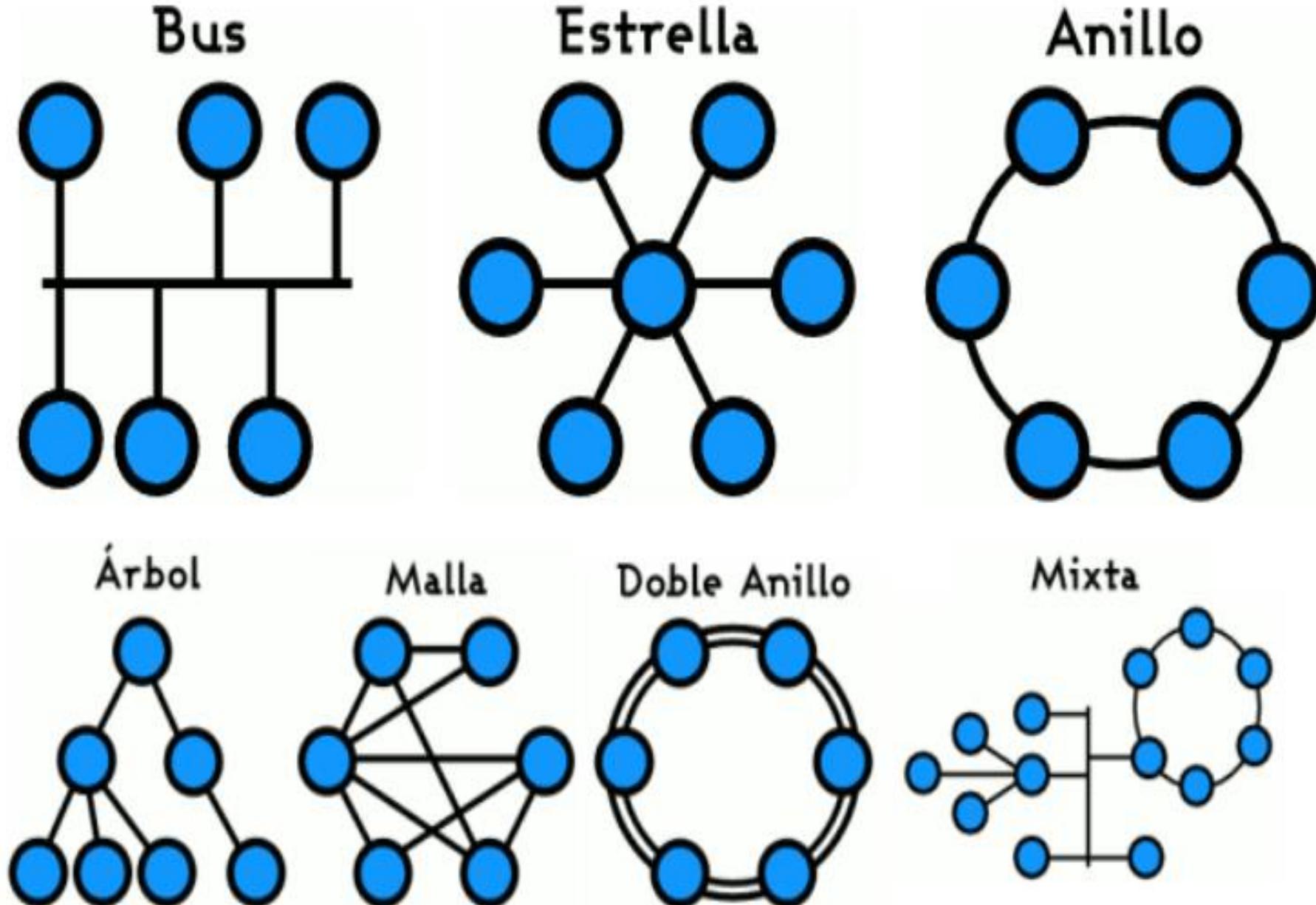
- **Redes cliente-servidor**, se basan en la existencia de uno o varios servidores, que darán servicio al resto de ordenadores que se consideran clientes. Este tipo de redes facilitan la **gestión centralizada**. Para crear redes de este tipo necesitamos sistemas operativos de tipo servidor, como Windows Server o GNU-Linux. Cabe destacar que en principio cualquier distribución Linux pueden actuar como servidor, aunque existen distribuciones especialmente recomendadas para este cometido, tales como Debian, Ubuntu Server, Red Hat Enterprise, etc.

Una computadora con software de servidor puede **prestar servicios a uno o varios clientes simultáneamente**.

Además, **una sola computadora puede ejecutar varios tipos de software de servidor**. En una oficina pequeña, puede ser necesario que una computadora actúe como servidor de archivos, servidor Web y servidor de correo electrónico, etc.



- Según la **Forma de conectar** los ordenadores, lo que se conoce por **topología**.
  - en Bus
  - en Anillo
  - en Estrella
  - en Árbol
  - en Malla
  - Doble anillo
  - Mixta
  - Totalmente conexa

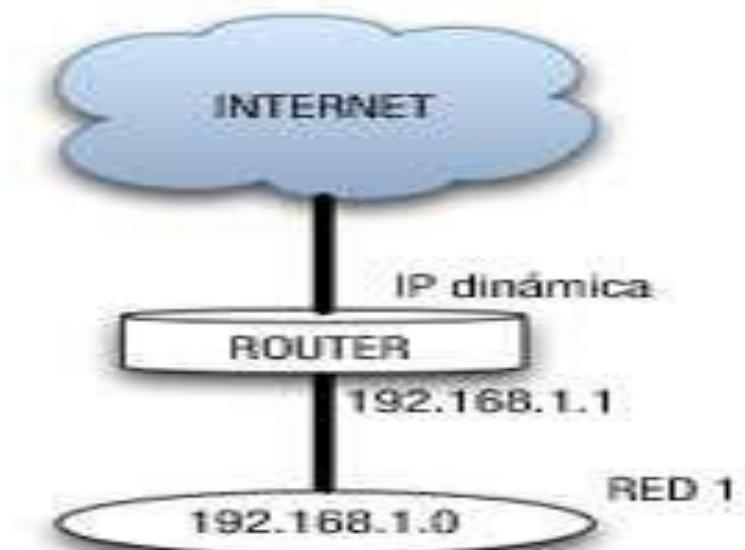


La topología de red se define como la **cadena de comunicación usada por los nodos que conforman una red para comunicarse**. Puede referirse, tanto al camino **físico** como al lógico.

- Usualmente usaremos topología desde el punto de vista **físico** y por tanto lo consideraremos como la **forma en que se conectan los ordenadores de una red**. Cuando se hace una instalación de red es conveniente **realizar un esquema** de red donde se muestre la ubicación de cada ordenador, cada equipo de interconexión e incluso del cableado. Se suele hacer **utilizando los planos del edificio o planta**, donde está ubicada la red y es una herramienta útil a la hora del mantenimiento y actualización.
- La topología lógica o **esquema lógico**, nos **muestra el uso de la red**, el nombre de los ordenadores, las **direcciones**, las **aplicaciones**, etc. En estos esquemas un grupo de ordenadores puede estar representado con un sólo icono.

Tenemos un gráfico donde se muestra un red de ordenadores que tendrá conexión a Internet gracias a un router.

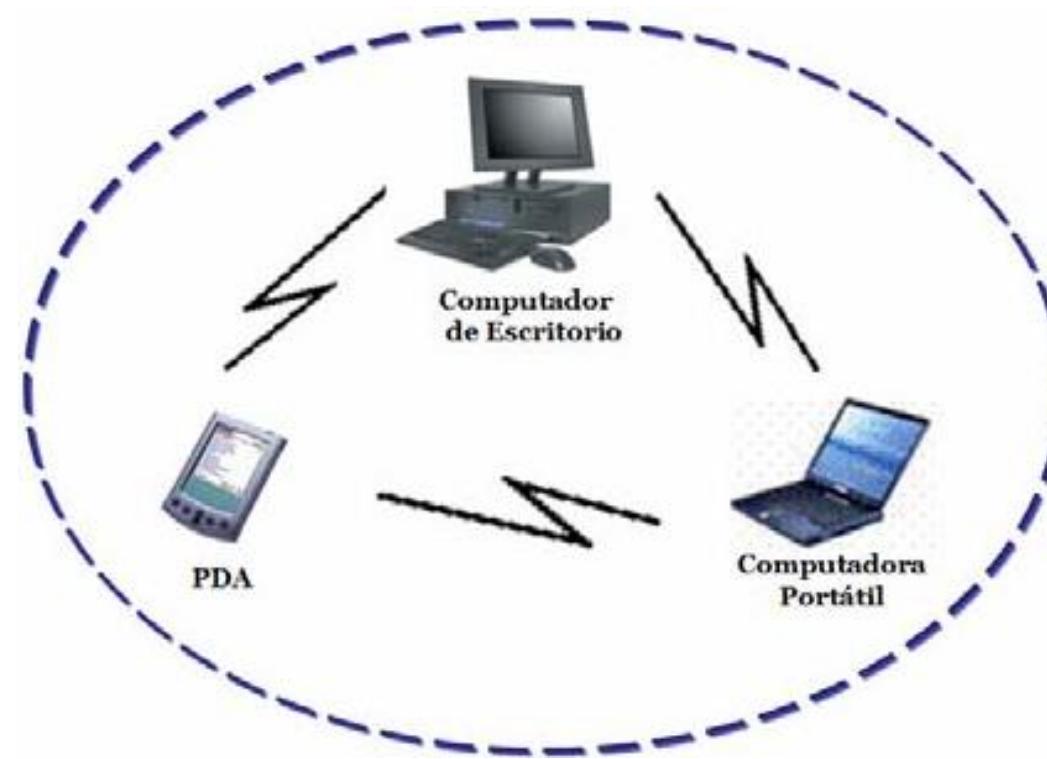
La red se representa con un óvalo donde dentro tiene la dirección de red y fuera el nombre de la red.



Otro concepto relacionado con la forma de conectar los ordenadores en red, es el de **modo de conexión**, este concepto está relacionado con las **redes inalámbricas**, representa **cómo se pueden conectar ordenadores en red de forma inalámbrica**

Dos modos de conexión inalámbrico:

- Modo **infraestructura**: Suele incluir un punto de acceso.
- Modo **ad-hoc**: No necesita punto de acceso. Es un tipo de red inalámbrica descentralizada. Permite la adhesión de nuevos dispositivos, con el solo hecho de estar en el rango de alcance de un nodo ya perteneciente a la red establecida.



## Bus.

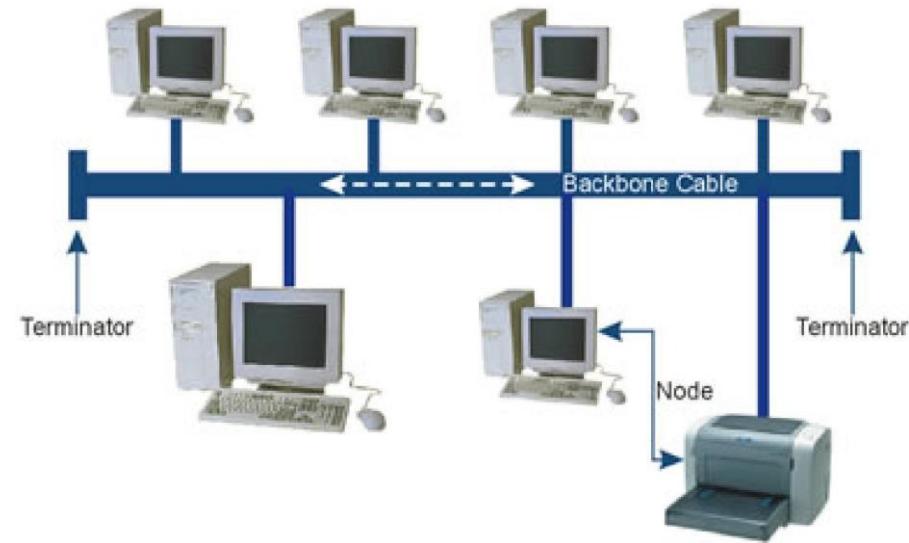
Usa un cable con cada ordenador conectado al **backboney terminadores** (en extremos) para evitar reflexiones.

Ventajas:

- **Facilidad de configurar** y facilidad de **crecimiento**.
- **Económicas**

Inconvenientes:

- **Complejidad de reconfiguración** y **aislamiento de fallos**.
- Un problema en el canal usualmente degrada toda la red.
- **Desempeño** disminuye a medida que la red crece.
- Altas **pérdidas** en la transmisión debido a **colisiones** entre mensajes.



## Anillo.

Esta topología se utiliza en las redes FDDI o Fiber Distributed Data Interface (Interfaz de datos distribuidos por fibra), que puede usarse como parte de una red troncal que distribuye datos por fibra óptica. En algunas configuraciones de servidores también se utiliza este tipo de topología. Conecta cada ordenador o nodo con el siguiente y el último con el primero, creando un **anillo físico de conexión**.

- Cada estación tiene un **receptor** y un **transmisor** que hace la función de **repetidor**, pasando la señal a la siguiente estación.
- Comunicación por el paso de un **testigo**, de esta manera se evitan eventuales pérdidas de información debidas a colisiones.
- Topologías de **anillo doble** donde dos anillos permiten que los datos se envíen en **ambas direcciones**. Crea **redundancia** (tolerancia a fallos).
- Cableado más complejo por mayor coste del cable, así como a la necesidad de emplear unos dispositivos denominados Unidades de Acceso Multiestación (MAU).
- Adición de nuevas estaciones no supone una complicación excesiva.



## En Estrella.

Las redes de área local modernas basadas en el estándar IEEE 802.3 utilizan esta topología.

- Existe un **nodo central**, al cual se conectan todos los equipos. Este nodo central puede ser: un router, un switch, o un hub. Canaliza toda la información y por el pasan todos los paquetes de usuarios, realizará funciones de **distribución, conmutación y control**.
- **Inconveniente:**
  - si el nodo central falla, toda la red fallaría.
- **Ventajas:**
  - fácil de instalar
  - muy escalable (es fácil agregar y quitar dispositivos finales)
  - fácil resolución de problemas.



- Un ampliación de la topología en estrella es la estrella extendida o **árbol** donde las **redes en estrella se conectan entre sí**.
- Cuando la estrella extendida tiene un **elemento de donde se parte**, hablaremos de la topología en **estrella jerárquica**, donde a partir de redes conectadas en estrella conseguimos una red más amplia y que mantiene una jerarquía de conexiones, ya que tenemos un nodo que es el inicio de la jerarquía. Este nodo suele ser un **router** y a partir de él se crea una red de área local que permite **dar servicios a redes de área locales más pequeñas**.

Este tipo de topologías es muy típica en redes de área local donde el principio de la jerarquía.

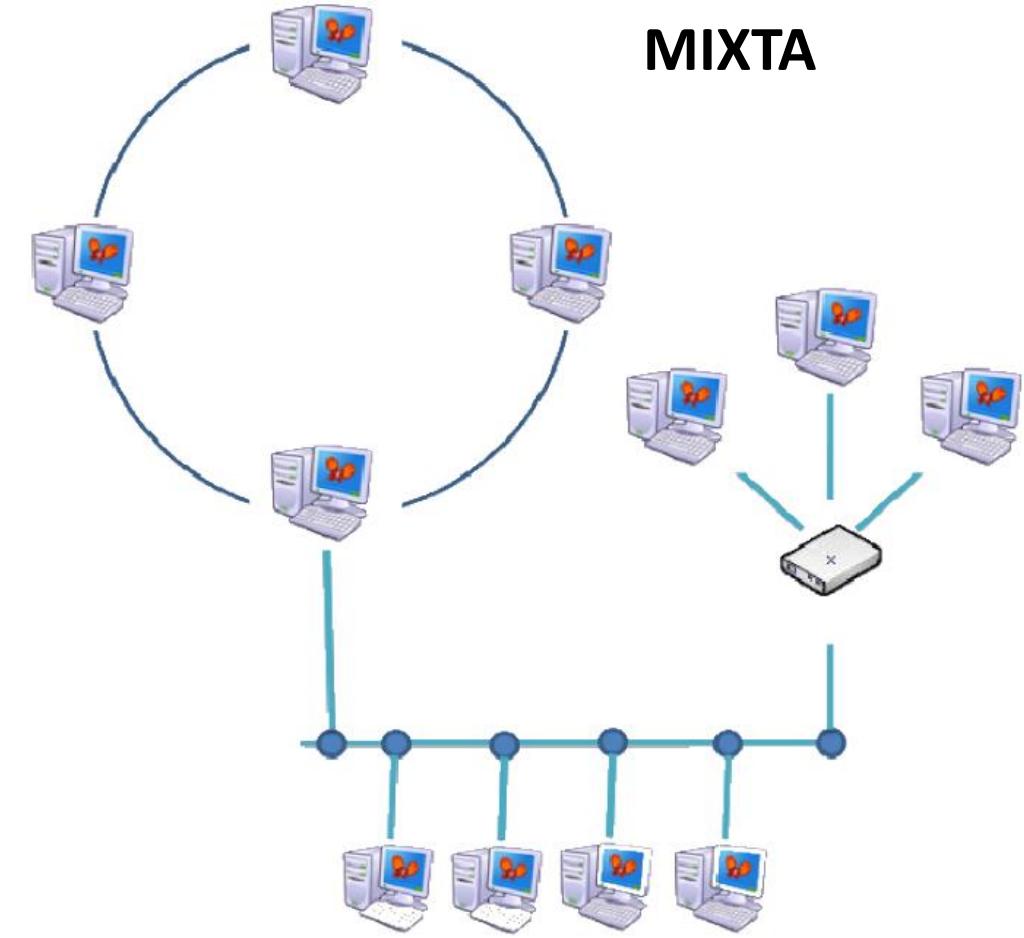
- El **router** que conecta a Internet, usualmente el que nos pone la compañía de Telecomunicaciones
- Los **switch** que dan servicio a diferentes aulas, salas de ordenadores, despachos, etc.

#### **Ventaja:**

- a partir de una única conexión a Internet podemos dar servicio a varias redes o subredes locales, con lo que ahorramos costes.

#### **Desventaja:**

- si el equipo de interconexión de mayor jerarquía falla, la red ya no presta los servicios para los cuales fue diseñada.



Relaciona cada concepto con su definición:  
Relacionar topologías y modos de conexión.

Concepto	Relación	Definición
Topología física		1. Esquema de conexión que muestra algunas características de la conexión.
Topología lógica		2. Modo de conexión inalámbrico, especialmente pensado para un propósito específico.
Modo infraestructura		3. Forma de conectar los ordenadores de una red.
Modo ad-hoc		4. Modo de conexión para ordenadores inalámbricos, que utiliza punto de acceso.

**Lo que caracteriza al modo infraestructura es:**

- Que todos los ordenadores se pueden conectar a Internet.
- Que todos los ordenadores pueden compartir información de forma inalámbrica.
- Que todos los dispositivos inalámbricos se conectan a través de un punto de acceso.

- Según el **tipo de conexión** podemos tener:

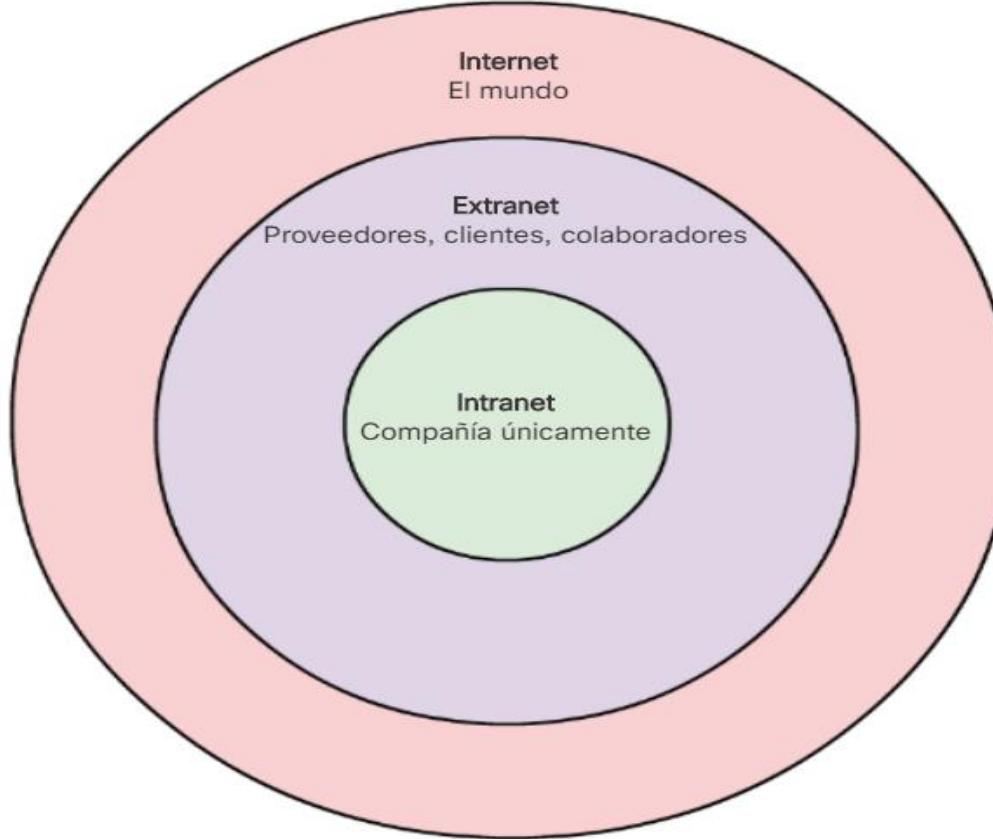
- Redes **cableadas**: En este tipo de redes se **utilizan diferentes tipos de cables para conectar** los ordenadores, más adelante estudiaremos lo relacionado con los tipos de cables más utilizados.
- Redes **inalámbricas**: Son las redes que no necesitan cables para comunicarse, existen diferentes tecnologías inalámbricas que más adelante estudiaremos.



- Otra clasificación interesante es **teniendo en cuenta el grado de difusión**, en esta clasificación distinguimos dos tipos de redes:
  - **Intranet** es una red de computadoras que utiliza alguna **tecnología de red para usos comerciales, educativos o de otra índole de forma privada**, esto es, que no comparte sus recursos o su información con otras redes, a no ser que autentifiquen, o cumplan unas medidas de seguridad determinadas.
  - **Internet** es un **conjunto descentralizado de redes de comunicación interconectadas** que utilizan la familia de **protocolos TCP/IP**, garantizando que las **redes físicas heterogéneas** que la **componen** funcionen como una **red lógica única**, de alcance mundial. Precisamente esta característica, es la que ha hecho que el uso de Internet se generalice y que todas las redes funcionen utilizando protocolos TCP/IP.

*El término **Internet** lo utilizamos para referirnos a la red informática mundial, descentralizada, formada por la conexión directa entre computadoras u ordenadores mediante un protocolo especial de comunicación. Para conocer más sobre esta red global:*

<http://es.wikipedia.org/wiki/Internet>



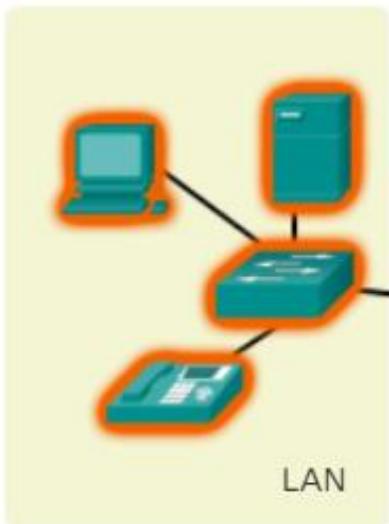
***¿Qué tipos de redes pueden considerarse si tenemos en cuenta el lugar en que se instalan o la zona a la que prestan servicios?***

- *Intranet e Internet.*
- *Red de área local, red área metropolitana y red de área amplia.*
- *Cableadas e inalámbricas.*
- *Bus, anillo y estrella.*

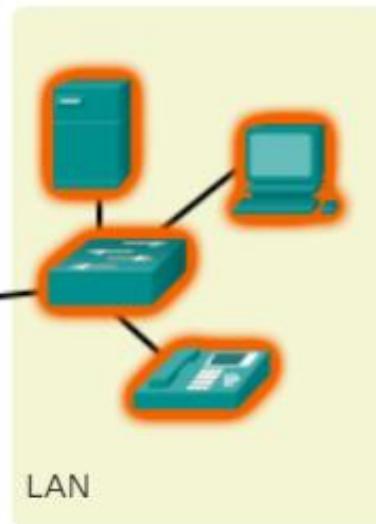
**La infraestructura de red contiene las siguientes categorías de componentes de red:**

- Dispositivos
- Medios

Dispositivos



Dispositivos



LAN

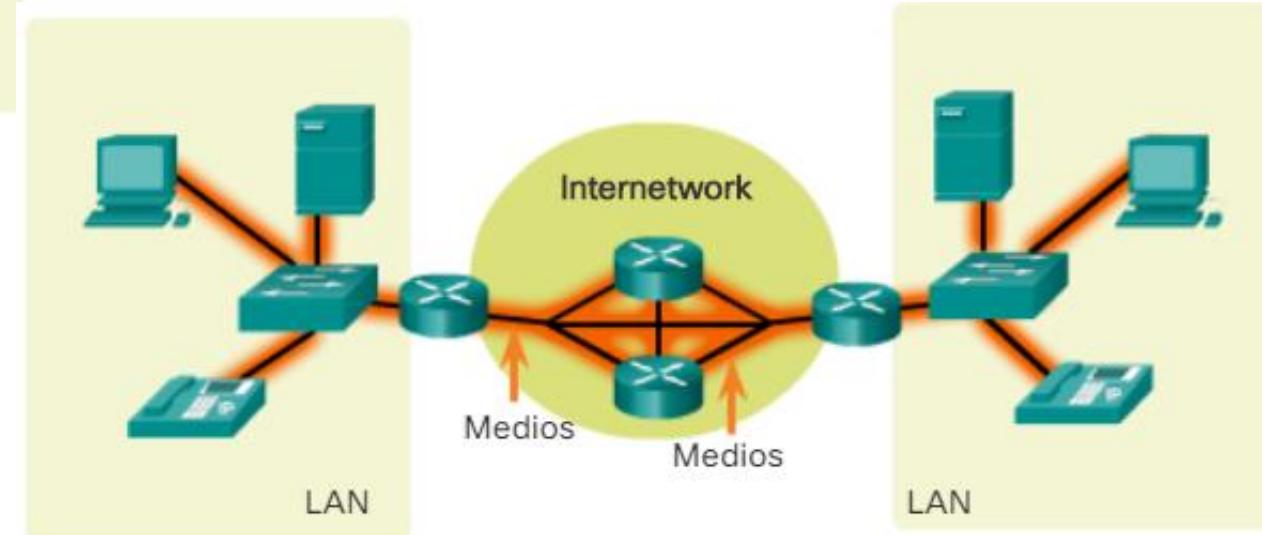
Internet  
Dispositivos  
Dispositivos

LAN

Medios  
Medios

LAN

Internet



## Dispositivos finales.

Son los dispositivos de red con los que las **personas están más familiarizadas**, también conocidos como “hosts”. Forman la interfaz entre los usuarios y la red de comunicación subyacente.

Un dispositivo host es el **origen o el destino de un mensaje transmitido a través de la red**.

Para **distinguir** un host de otro, cada host en la red se identifica por una **dirección**. Cuando un host inicia la comunicación, utiliza la dirección del host de destino para **especificar a dónde se debe enviar** el mensaje.

- Computadoras (estaciones de trabajo, computadoras portátiles, servidores de archivos, servidores web)
- Impresoras de red
- Teléfonos VoIP
- Cámaras de seguridad
- Dispositivos portátiles móviles (como smartphones, tablet PC, PDA y lectores inalámbricos de tarjetas de débito y crédito, y escáneres de códigos de barras)



## Dispositivos intermedios.

Los dispositivos intermediarios **interconectan dispositivos finales**. Estos dispositivos proporcionan conectividad y operan detrás de escena para asegurar que los **datos fluyan a través de la red**. Los dispositivos intermediarios conectan los hosts individuales a la red y pueden conectar varias redes individuales para formar una internetwork.

Estos dispositivos utilizan la dirección host de destino, conjuntamente con información sobre las interconexiones de la red para **determinar la ruta que deben tomar los mensajes** a través de la red.

- Acceso a la red (switches y puntos de acceso inalámbrico)
- Internetworking (routers)
- Seguridad (firewalls)



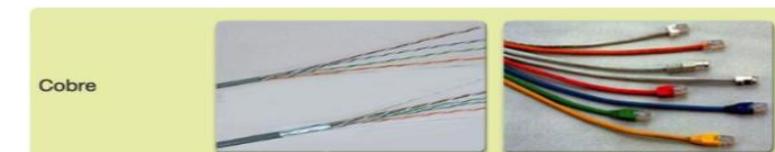
# Medios de red

La **comunicación** a través de una red es **transportada por un medio**. El medio proporciona el **canal** por el cual **viaja el mensaje** desde el origen hasta el destino.

La **codificación** de la señal que se debe realizar para que se transmita el mensaje es diferente para cada tipo de medio.

No todos los **medios** de red tienen las mismas **características** ni son adecuados para el mismo fin. Los **criterios** para elegir medios de red son los siguientes:

- La **distancia** por la que los medios pueden transportar una señal correctamente
- El **entorno** en el que se instalarán los medios
- La cantidad de datos y la **velocidad** a la que se deben transmitir
- El **costo** del medio y de la **instalación**



- Hilos metálicos dentro de cables
- Fibras de vidrio o plástico (cable de fibra óptica)
- Transmisión inalámbrica

La **codificación** de la señal que se debe realizar para que se transmita el mensaje es diferente:

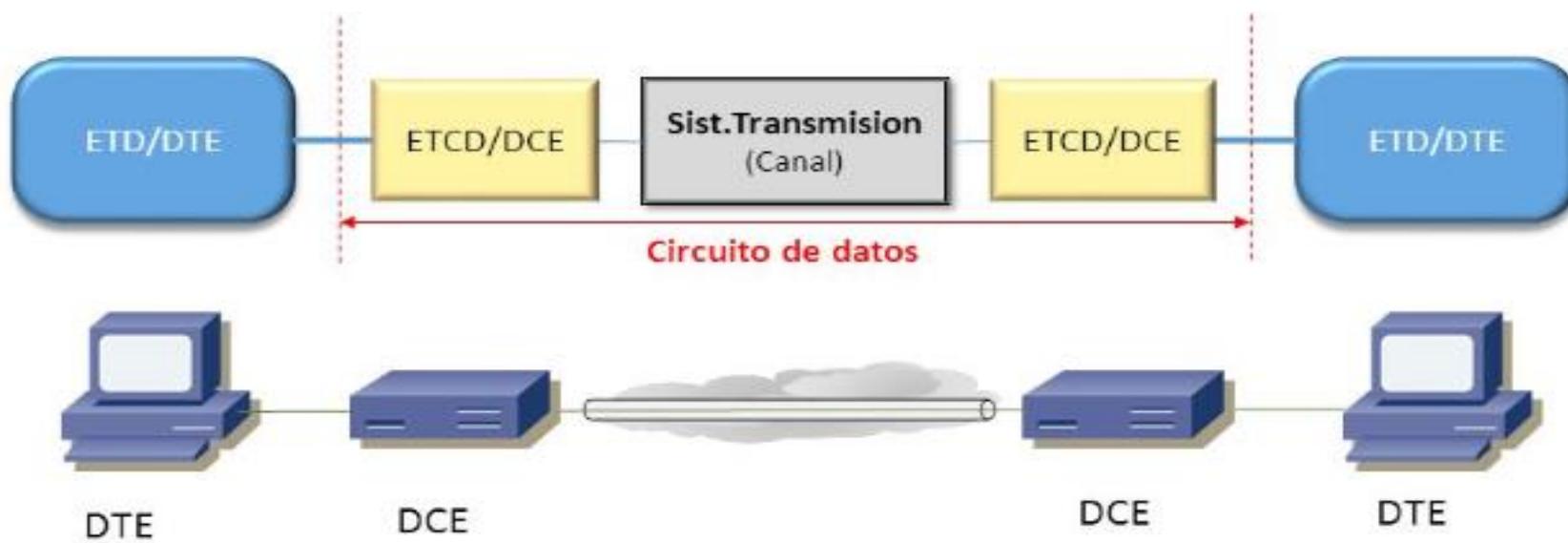
- En los hilos metálicos, los datos se codifican dentro de **impulsos eléctricos**.
- Las transmisiones por fibra óptica dependen de **pulsos de luz**, dentro de intervalos de luz visible o infrarroja.
- En transmisiones inalámbricas, **patrones de ondas electromagnéticas** son los distintos valores de bits.

Los conceptos relacionados con los **componentes de red** son:

- **Equipo Terminal de Datos (ETD):** que serán todos los equipos, ya sean emisores o receptores de información.
- **Equipo de Comunicación de Datos (ECD):** que es cualquier dispositivo que participa en la comunicación pero que no es ni emisor original ni receptor final.

Podrás aclarar los conceptos estudiados en este apartado, además de conocer algunos conceptos que desarrollaremos durante este curso.

<http://www.slideshare.net/mamogetta>



# Redes de ordenadores. Ventajas.

**Red de ordenadores o red informática:** es un **conjunto de equipos informáticos conectados** entre sí por **medio** de dispositivos físicos que **envían y reciben** impulsos eléctricos, ondas electromagnéticas o cualquier otro medio para el **transporte de datos** con la finalidad de:

- **compartir los recursos y la información**
- asegurar la **confiabilidad** y la **disponibilidad** de la información
- aumentar la **velocidad de transmisión** de los datos
- **reducir el coste general** de estas acciones.
- aumentar las **posibilidades de colaboración**.
- facilitar la **gestión centralizada**.

La idea principal de las redes, es, que, a medida que conectamos más dispositivos y estos comparten sus recursos, la **red será más potente**. Es **mejor que hacerlo de forma aislada**.

*De las siguientes afirmaciones elige las que sean correctas:*

- *Siempre que montemos una red de ordenadores reduciremos costes.*
- Si tenemos una red de ordenadores tenemos la posibilidad de compartir recursos.*
- *Siempre que los ordenadores estén en red podremos hacer una gestión centralizada de los mismos.*
- Los motivos principales para conectar ordenadores en red suelen ser compartir una conexión a Internet y compartir información.*

Cuando se habla de compartir **recursos**:

- La mayoría tenemos en mente la **conexión a Internet**. Es obvio que una sola conexión a Internet compartida es **más barata** que tener una conexión para cada ordenador.
- La **utilización de periféricos compartidos** tales como: impresoras, discos duros de red, escáneres, etc.
- Posibilidad de **compartir software**. El software compartido cada vez es mayor, y en algunos entornos de trabajo es indispensable.

Cuando se habla de compartir **información**:

- Podemos usar **bases de datos** compartidas, documentos que pueden leerse, e incluso elaborarse por varios usuarios y usuarias diferentes.

Cuando compartimos recursos e información, las posibilidades de **colaboración** aumentan.

- Esa colaboración puede darse entre personas que estén en la misma oficina o instituto, pero también se puede dar entre personas que estén tan alejadas que ni siquiera lleguen a conocerse >>> **computación en la nube** para referirse a la posibilidad de ofrecer servicios informáticos a través de Internet.

Respecto a la **gestión centralizada** de los recursos:

- Mejora la seguridad de los sistemas.
- Suele optimizar las prestaciones de la red y sale más barato.

Podemos decir que el **principal objetivo** de cualquier asociación, corporación o persona es, que **cuando haga una inversión**, ésta no sea excesiva. Si se hace una buena planificación de la red, y se hace un buen diseño de la misma, seguro que se **reducirán costes de implantación y mantenimiento**.

## Técnicas de Conmutación.

Las **redes conmutadas** son aquellas que **precisan de una conmutación entre los nodos** para establecer las rutas adecuadas.

Las **redes WAN basan su funcionamiento en las técnicas de conmutación**. Podemos definir las técnicas de conmutación como la **forma en que un usuario y otro establecen la comunicación**.

Técnicas:

- **Commutación de circuitos:**

Consiste en el **establecimiento de un enlace físico para la transmisión entre dos nodos**, que se **liberará** cuando termine la comunicación en el caso de utilizar una red conmutada, o permanecerá si se utiliza una red dedicada. Al establecerse los **datos que forman el mensaje se transmiten secuencialmente** siguiendo el mismo circuito.

Principales **tecnologías**: RTB/RDSI/DSL

(Ejemplo: transmisión de datos a través de la red telefónica conmutada).

**Desventaja:** este camino no se comparte con otros usuarios, es exclusivo, por lo que es posible que se esté **infrautilizando** el canal.

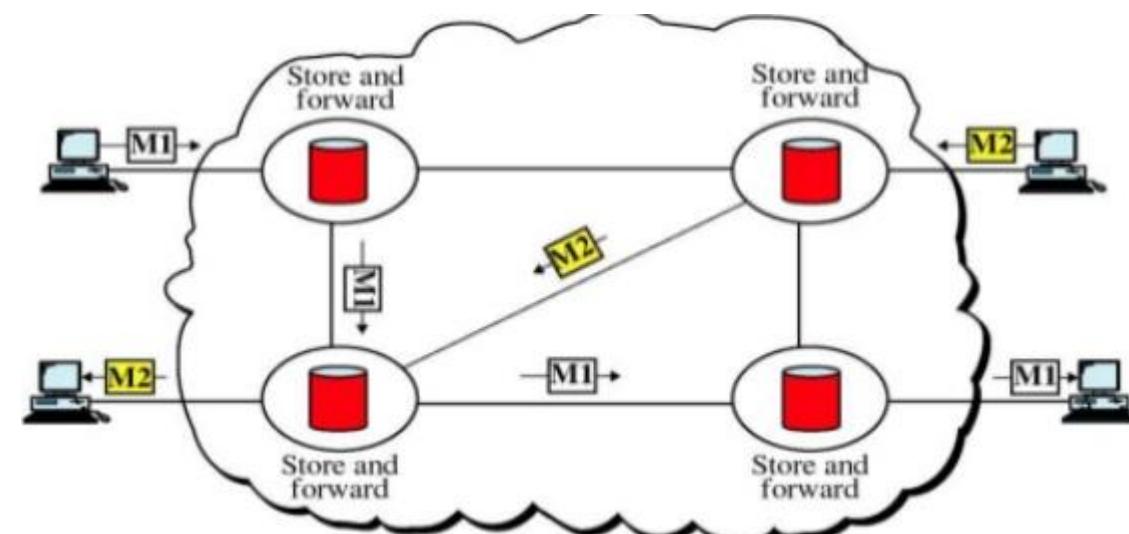
- **Commutación de mensajes:**

Es un método basado en el tratamiento de **bloques de información**, dotados de una dirección de origen y otra de destino, de esta forma la red almacena los **mensajes** hasta verificar que han llegado correctamente a su destino y proceden a su retransmisión o destrucción. Es una técnica empleada con el servicio télex y en algunas de las aplicaciones de correo electrónico.

El emisor **envía todo el mensaje completo** hacia un nodo intermedio que lo **almacena** hasta que llegue su turno para enviarlo al siguiente nodo/receptor.

### Desventajas:

- Nodos intermedios requieren de una **gran capacidad** de almacenamiento.
- En caso de error en la transmisión es necesario **reenviar** todo el mensaje.



- **Commutación de paquetes:**

Es la forma de trasmisión que se **utiliza en Internet**.

Consiste en **dividir** el mensaje en **paquetes**. Cada paquete es enviado de un **nodo de la red al nodo siguiente**. Cuando el nodo receptor recibe completamente el paquete, lo almacena y lo vuelve a emitir al nodo que le sigue. Este proceso se va repitiendo **hasta que el paquete llegue al destino final**.

Es la más ampliamente utilizada para conectar redes. Los nodos **no necesitan una gran capacidad de almacenamiento** y el **tráfico por la red es más fluido**.

Principales tecnologías: Frame Relay – ATM.

Es importante que conozcan los conceptos relacionados con la commutación de paquetes, ya que es la base del funcionamiento de Internet. Para ello debes leer el artículo de wikipedia relacionado con este tema:

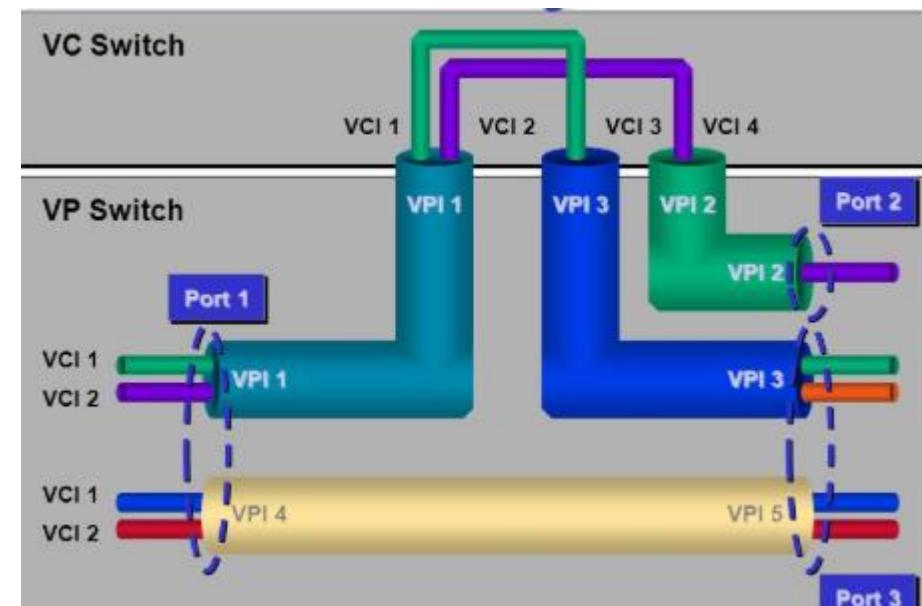
[http://es.wikipedia.org/wiki/Commutaci%C3%B3n\\_de\\_paquetes](http://es.wikipedia.org/wiki/Commutaci%C3%B3n_de_paquetes)

Para la utilización de la conmutación de paquetes se han definido dos tipos de técnicas:

- los **datagramas** (Internet), **no orientado a la conexión**, envío de paquetes **sin establecimiento previo de circuito** físico/virtual. En destino los paquetes pueden **no llegar** o hacerlo de forma **desordenada**.
- los **circuitos virtuales**, **orientado a la conexión**, existe una **conexión lógica (CV)** entre **origen y destino**, los paquetes siguen una **camino determinado sobre un canal físico**.

Puede haber **varios canales lógicos**:

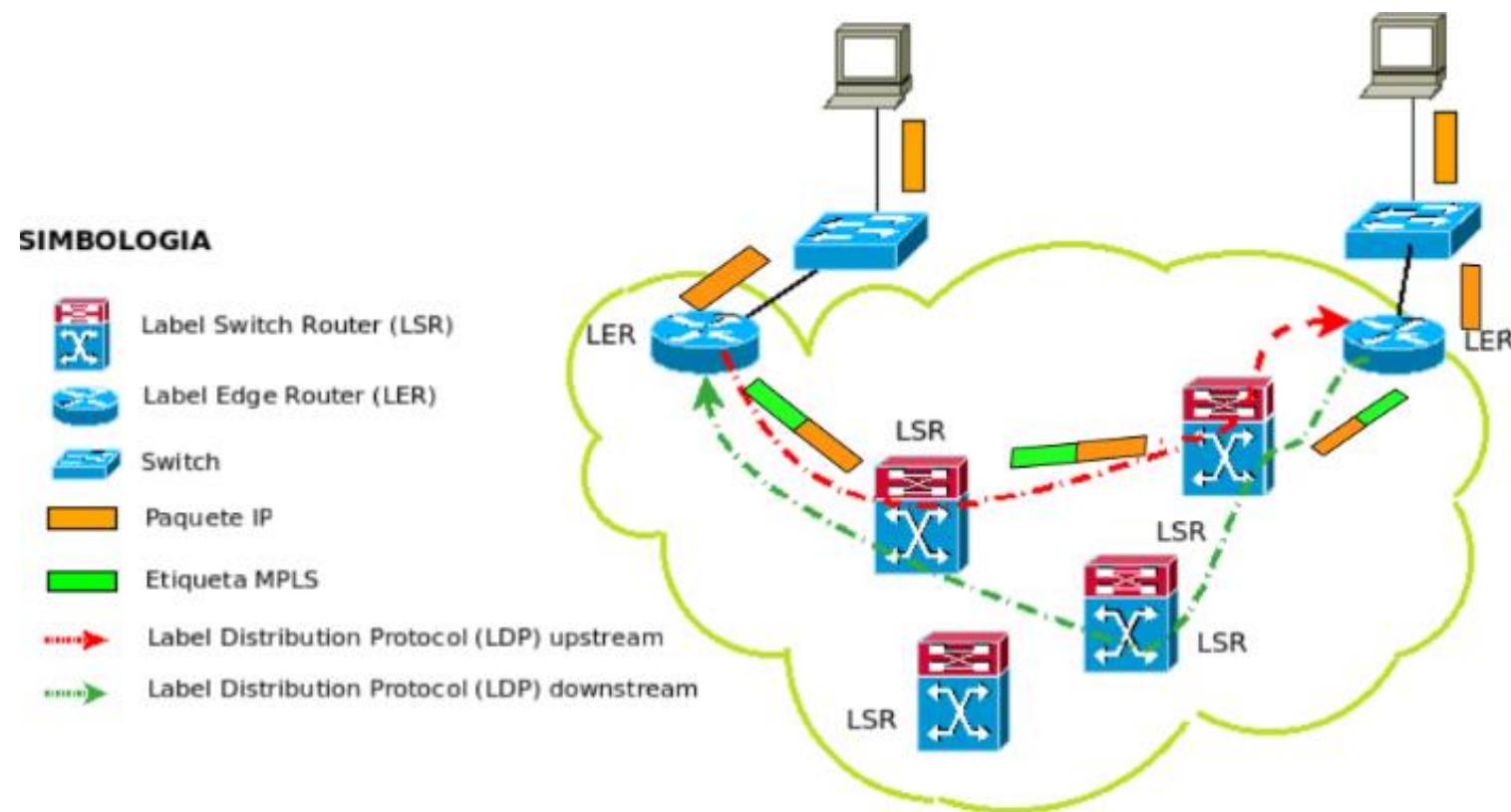
- **Circuitos Virtuales Permanentes (CVP)**: no hay establecimiento porque ya lo ha habido previamente, la transmisión sería equivalente a una línea punto a punto.
- **Circuitos Virtuales Comutados (CVC)**: hay **establecimiento previo** y puede hacerse con un extremo distinto cada vez.



- **Commutación de etiquetas (MPLS):**

- Surge para aumentar la velocidad de transferencia de la información.
- Mayor rendimiento, mayor flexibilidad y fiabilidad para la transmisión de datos de alta velocidad.

MPLS asigna una **etiqueta a cada paquete**. De esta forma la retransmisiones no necesitan inspeccionar el paquete completamente, únicamente la **etiqueta** asociada, ganando velocidad. Se crean **circuitos extremo a extremo para grupos de paquetes** en lugar de paquetes individuales.



Las redes de área extensa (WAN) suelen estar **soportadas** por redes públicas de telecomunicaciones que solemos usar para conectarnos a Internet.

Ejemplos de estas redes serán:

- La **red telefónica básica** o **red telefónica conmutada** (RTB):

Permite que hablemos por teléfono, pero si utilizamos un **módem** podemos transmitir datos a baja velocidad.

- El **bucle de abonado digital asimétrico**:

Conocido como **ADSL**, la operadoras de telefonía ofrecen la posibilidad de utilizar una **línea de datos independiente**, aprovechando el ancho de banda disponible por encima del requerido por el servicio telefónico hasta el límite permitido por la propia línea.

- **Telefonía móvil**:

Proporcionan la posibilidad de **transferir tanto voz y datos** (una llamada telefónica o una video llamada) y datos (descarga de programas, correo electrónico, y mensajería instantánea).

- **Internet por cable**:

Usando **cable módem o enrutadores**, las redes de cable ofrecen la posibilidad de utilizar cable de fibra óptica combinado con cable coaxial, para dar una alta velocidad en el acceso a Internet.

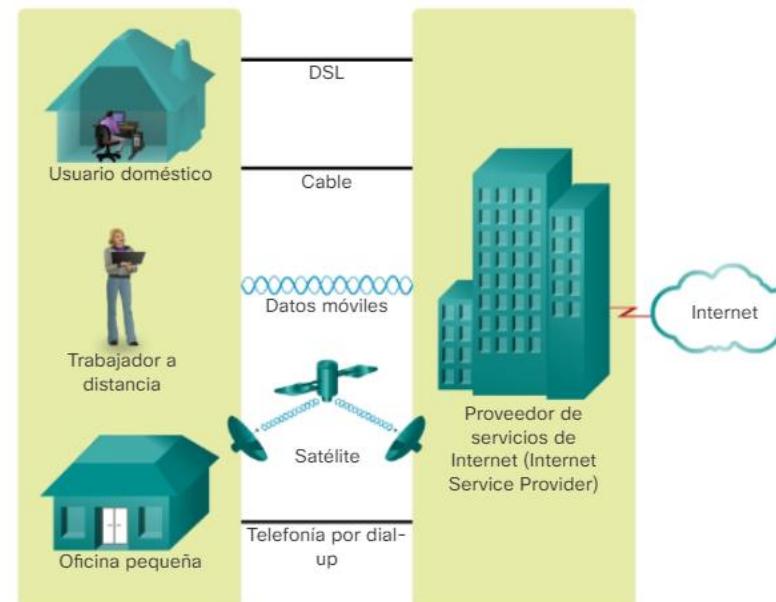
- **Satelital:**

Las **antenas parabólicas** requieren una línea de vista despejada al satélite, por lo que no son adecuadas para zonas muy boscosas o lugares que posean algún otro tipo de obstrucción aérea.

Las **velocidades varían** según el contrato, pero suelen ser buenas.

Los **costos de equipos e instalación pueden ser elevados.**

Una gran **ventaja** para las **áreas que no tienen acceso a otro tipo** de conectividad a Internet.



Si quieres conocer más sobre las redes WAN recomendamos el siguiente documento en formato de presentación, donde se hace un exhaustivo repaso a todo lo que tiene que ver con la redes WAN. Se recomiendan especialmente las diapositivas de la 45 a la 81 donde se explican las tecnologías WAN.

<http://es.scribd.com/doc/13257660/Tecnologias-WAN>

## Actividad para Clase.

Dibuja tú propio concepto de Internet:

### Objetivos

Las redes constan de varios componentes diferentes. Dibuja y rotula un mapa de Internet tal como la interpretas en el presente. Incluye ubicaciones como tú casa, lugar de estudios o trabajo, y del cableado, los equipos y los dispositivos correspondientes, entre otros.

Puedes incluir algunos de los siguientes **elementos**:

- Dispositivos o equipos.
- Medios (cableado).
- Proveedores de servicios de Internet.



# La arquitectura de red.

## El concepto de arquitectura de red es:

- **más amplio que pensar como está construida la red, los cables, los equipos, etc.**
  - **incluye cuestiones relacionadas con el hardware y con el software de una red.**

Es conveniente entender que uno de los **problemas** más importantes a la hora de diseñar una red **no es que los equipos se conecten entre sí**, si no que estos equipos **puedan comunicarse, entenderse, compartir recursos**, que al fin y al cabo es lo que pretendemos.

Para esto ya hemos mencionado que se necesitan unos **protocolos de comunicaciones**.

Debido a la **complejidad** que acarrea considerar la red como un todo, se consideró oportuno **organizar las redes como una serie de capas**, donde cada capa se ocuparía de **alguna función**. De esta forma se **reduciría la complejidad del diseño de la red** y de las **aplicaciones** que en ella se utilicen.



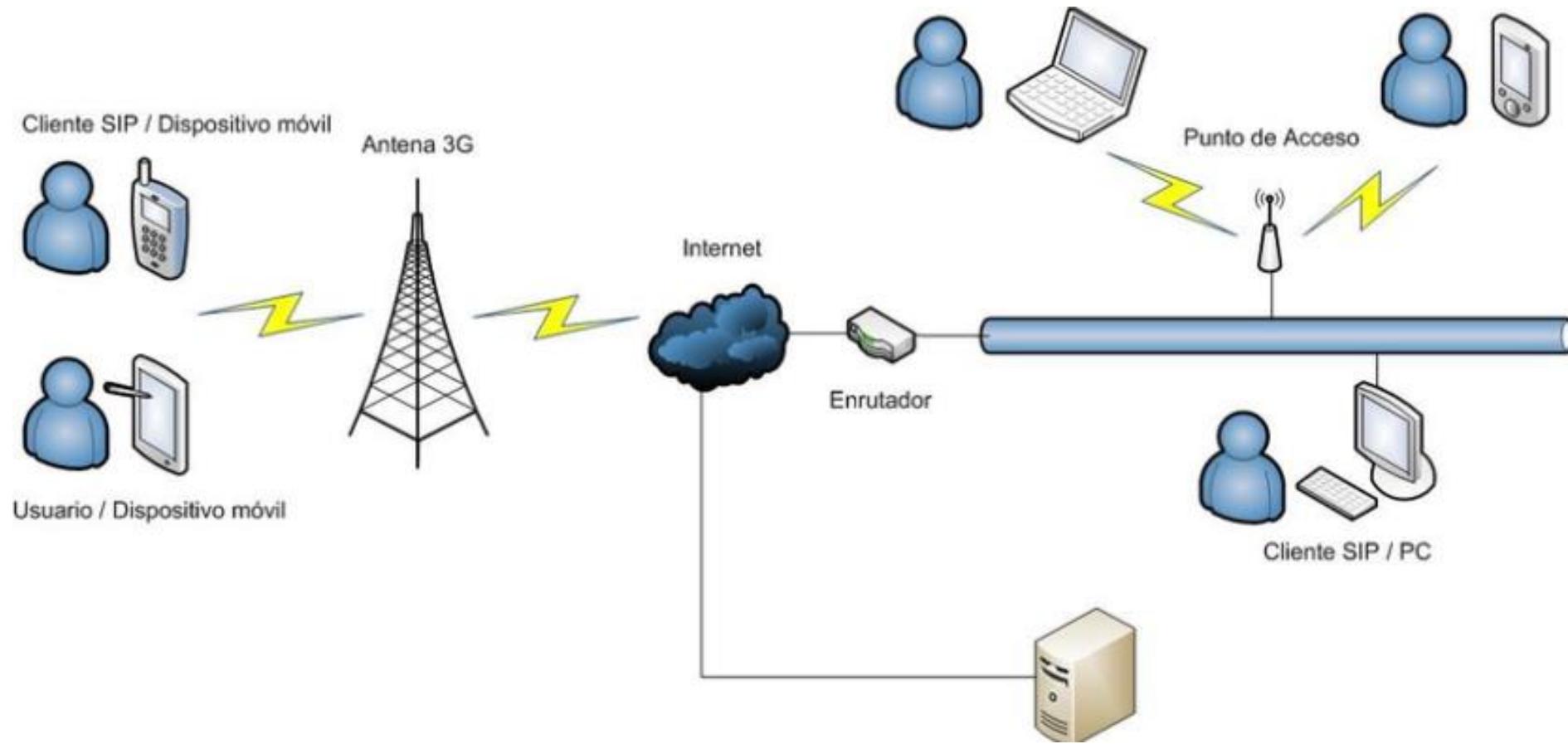
Por tanto podemos **definir arquitectura de red** como:

- **conjunto de capas o niveles**
- **protocolos definidos en cada una de estas capas**, que hacen posible que un **ordenador** se **comunique con otro ordenador independientemente** de la red en la que se encuentre

Esta definición implica, que la **especificación** de una arquitectura de red debe incluir información suficiente para que cuando se **desarrolle un programa o se diseñe algún dispositivo**, **cada capa responda de forma adecuada al protocolo apropiado**.

La **arquitectura de red** tendrá que **tener en cuenta al menos tres factores importantes**:

- La **forma** como se conectan los nodos de una red, que suele conocerse como **topología**, además de las **características físicas** de estas conexiones.
- La **manera de como compartir información** en la red, que en algunos casos obligará a elegir un **método de acceso a la red** y unas reglas para evitar perdida de información.
- Unas **reglas generales** que no sólo **favorezcan** la comunicación, si no que la **establezcan, mantengan** y permitan la utilización de la información, estas reglas serán los **protocolos** de comunicación.



## *¿Cuales son los tres factores principales para definir una arquitectura de red?*

- *El cableado, las conexiones y los ordenadores.*
- *Las aplicaciones, los protocolos que usan estas aplicaciones y las conexiones.*
- *La topología, el método de acceso a la red y los protocolos de comunicaciones.*

## Modelo por capas o niveles.

Hemos comentado que la **arquitectura de red**:

- se **dividía por niveles o capas** para **reducir la complejidad** de su diseño.

Esta división por niveles **conlleva** que:

- cada uno de estos **niveles tenga** asociados, **uno o varios protocolos** que **definirán las reglas de comunicación** de la capa correspondiente.

Por este motivo, también se utiliza el término **pila de protocolos** o **jerarquía de protocolos** para definir a la arquitectura de red que utiliza unos protocolos determinados.



Pero, ¿cómo funciona una arquitectura basada en niveles?.

En el gráfico podemos ver el esquema de una arquitectura de red de cuatro niveles.

Podemos observar:

- **dos ordenadores** que tendrán implementada la arquitectura,
- **cuatro niveles**, cada nivel tendrá **sus protocolos**, por lo que podemos decir que la comunicaciones entre niveles iguales se hace a través de los protocolos correspondientes.
- **flujo real de información**, los datos que queremos transmitir irán de un ordenador a otro **pasando por cada uno de los niveles**.

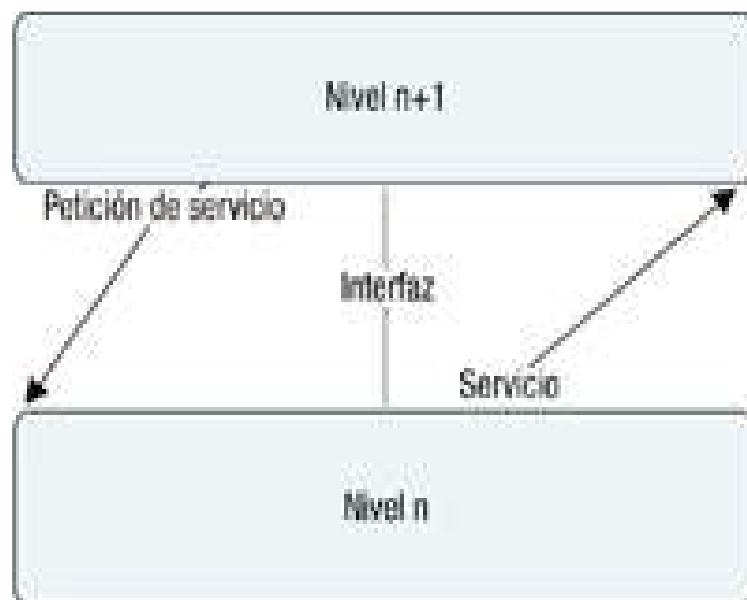
Esto implica que en la realidad los **datos no se transfieren directamente de una capa a otra del mismo nivel**, si no que:

- **cada capa pasa los datos e información de control a la capa adyacente**.
- la información **pasará por todas las capas**, se pasará al medio de transmisión adecuado y posteriormente sucederá lo mismo, pero en sentido contrario, en el otro ordenador.
- la **información llegará a su destino y cada nivel sólo se ocupará de los datos y la información de control que necesite, según el protocolo utilizado**, sin preocuparse de lo que hagan o necesiten los otros niveles.

Con esta forma de trabajar:

- Cada capa tiene unos **servicios asignados**.
- Las capas están **jerarquizadas** y cada una tiene unas **funciones**, de esta forma los niveles son **independientes entre sí**, aunque se **pasan los datos necesarios** de una a otra.
- Las capas adyacentes tienen lo que se llama una **interfaz**. En este contexto la interfaz **definirá las operaciones y servicios** que la capa inferior ofrece a la superior.

Cuando los diseñadores, diseñadoras, o fabricantes quieren fabricar productos compatibles, deben seguir los **estándares de la arquitectura de red**, para esto es importante **definir interfaces claras** entre niveles y que cada nivel tenga **bien definidos sus servicios**.



Para saber más sobre el modelo de Capas:

<https://pondalpar120.wordpress.com/2010/10/22/el-modelo-osi-historia-y-forma/>

**Recurso. Mostrar vídeo:**

¿Qué es una arquitectura de protocolos en Capas?

<https://youtu.be/oHJOo38Ts70>

Todo esto implica que para un **buen funcionamiento** de la red se deben, **respetar ciertas reglas**:

- los **servicios** se definen mediante **protocolos estándares**
- **cada nivel** sólo se comunique con el nivel **superior o el inferior**
- **nivel inferior proporciona servicios a su nivel superior.**

Hay que comentar que **este tipo de arquitectura** por niveles :

- **conlleva** cada nivel genera su **propio conjunto de datos**, ya que **cada capa pasa los datos originales junto con la información que ella genera**, para así poder controlar la comunicación por niveles.
- la información para los niveles inferiores se trata **como si fueran datos**, ya que **sólo la utilizará el nivel correspondiente del ordenador de destino**. Tendrá diferentes nombres.

Destacar que las arquitecturas de red basadas en capas:

- **facilitan las compatibilidades**, tanto de **software** como de **hardware**
- **facilitan modificaciones futuras**, ya que no es necesario cambiar todas las capas cuando queremos mejorar el sistema. Bastaría modificar los protocolos por niveles y podríamos conseguir mejoras en el sistema.

# Protocolo de comunicación.

Un protocolo de comunicaciones es un **conjunto de reglas normalizadas para la representación, señalización, autenticación y detección de errores** necesario para **enviar información a través de un canal de comunicación**.

Entre el conjunto de normalizaciones necesarias para poder establecer una comunicación **necesitamos** protocolos para:

- **Identificar** el emisor y el receptor.
- **Definir** el medio o **canal** que se puede utilizar en la comunicación.
- **Definir el lenguaje** común a utilizar.
- **Definir** la forma y estructura de los **mensajes**.
- Establecer la **velocidad y temporización de los mensajes**.
- Definir la **codificación y encapsulación del mensaje**.

Algunas **cuestiones** que los protocolos de redes deben resolver serán:

- **El enrutamiento:**

En las redes de ordenadores pueden **tenerse diferentes rutas para llegar a un mismo destino**, por tanto debe elegirse una de ellas, siendo deseable que siempre se elija la mejor o **más rápida**. Por tanto las arquitecturas de red, deben tener protocolos que sirvan para este fin, ya veremos **cuales son y en que nivel se resuelve**.

- **El direccionamiento:**

Dado que una red se compone de **muchos nodos** conectados entre sí, debe haber alguna **forma de conocer cual es cual**. Para esto necesitamos definir **direcciones de red** que permitan determinar a que ordenador me quiero conectar o por donde debo conectarme para llegar a un destino. Para poder conseguir esto, las arquitecturas de red definen protocolos de direccionamiento, **desde un punto de vista lógico y físico**, que se definen en niveles adecuados para que la comunicación sea posible, y no se produzcan duplicidades.

- **La necesidad de compartir un medio de comunicaciones:**

Puede darse el caso que **se comparta un mismo medio para transmitir**, por tanto deben establecerse **mecanismos** que controlen el **acceso al medio y el orden en el que se accede**.

- **La saturación:**

Los protocolos de cualquier nivel deben ser capaces de **evitar** que el **receptor** del mensaje, o los dispositivos **intermedios** que actúan en la transmisión del mensaje, se **saturen**. Esto suele ser un problema, y no siempre es fácil de resolver, pero un buen diseño y la adecuación de la red a las necesidades ayudan.

- **El control de errores:**

Es deseable que los protocolos de red tengan mecanismos de control de errores. Como veremos cuando analicemos las arquitecturas de red este control se puede hacer **desde diferentes puntos de vista y en diferentes niveles**.

Gracias a unos **protocolos estandarizados**, y a un buen diseño de red, podemos conseguir que **ordenadores de todo el mundo se comuniquen entre sí**.

*De los que hemos explicado podemos deducir que las características principales de los protocolos son:*

- *El emisor, el receptor y el mensaje.*
- *La identificación del emisor y el receptor.*
- *El direccionamiento y el enrutamiento.*
- *Mensaje, codificación, formato, tamaño del mensaje y temporización.*

# Funcionamiento de una arquitectura basada en niveles.

## Modelo OSI.

El **modelo OSI** (Open System Interconnection - Interconexión de Sistemas Abiertos), es el modelo de red creado por la **Organización Internacional para la Normalización (ISO)** en 1984. Este modelo:

- define un **marco de referencia** para la definición de arquitecturas de interconexión de sistemas de comunicaciones. No es una arquitectura desarrollada en ningún sistema. Se trata de un modelo teórico
- **simplifica las actividades de red** >>> agrupa los procesos de comunicación en **siete capas** que realizan tareas diferentes.

### ¿Porqué estudiar un modelo que no tiene implementación?

Aunque el modelo OSI no está realmente desarrollado en ningún sistema, **es conveniente conocerlo y aplicarlo**, ya que nos sirve para poder **entender los procesos** de comunicación que se producen en una red, para realizar una detección de errores o un plan de mantenimiento.

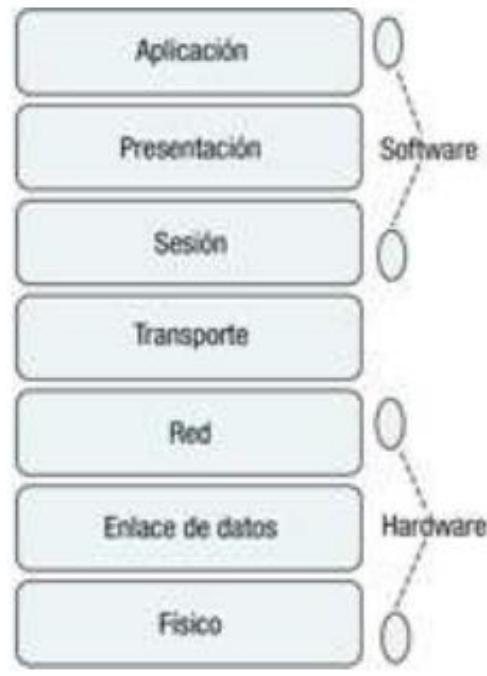
La representación gráfica del modelo OSI, suele hacerse como una **pila**:

- en lo más alto estaría la capa7 >>> **Aplicación**
- en lo más bajo la capa1 >>> **Física**

Mencionar que en ocasiones se hace **referencia** a que:

- Las capas 1-3 del modelo están relacionadas con el **hardware**
- Las capas 5-7 están relacionadas con el **software**
- La capa 4 una capa **intermedia** entre hardware y software.

Esto suele ser así por que los **dispositivos y componentes** de red, suelen trabajar en los niveles 1 a 3, siendo los **programas** los que trabajan en los niveles superiores.



## Física

Los protocolos de capa física describen los medios mecánicos, eléctricos, funcionales y de procedimiento para activar, mantener y desactivar conexiones físicas para la transmisión de bits hacia un dispositivo de red y desde él.

## Enlace de datos

Los protocolos de capa de enlace de datos describen los métodos para intercambiar tramas de datos entre dispositivos en un medio común.

## Red

La capa de red proporciona servicios para intercambiar los datos individuales en la red entre dispositivos finales identificados.

## Transporte

La capa de transporte define los servicios para segmentar, transferir y rearmar los datos para las comunicaciones individuales entre dispositivos finales.

## Modelo OSI

7. Aplicación

6. Presentación

5. Sesión

4. Transporte

3. Red

2. Enlace de datos

1. Física

## Sesión

La capa de sesión proporciona servicios a la capa de presentación para organizar su diálogo y administrar el intercambio de datos.

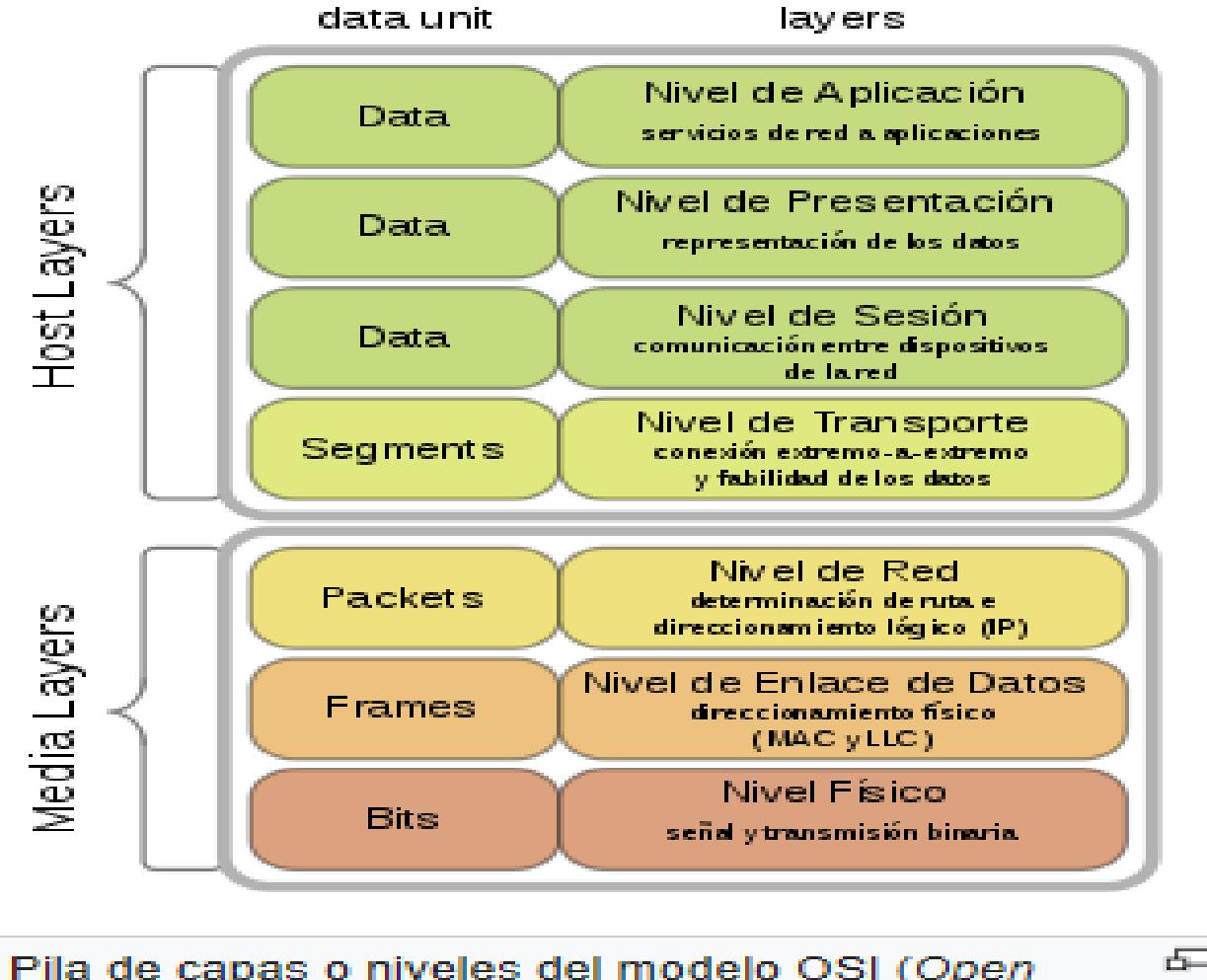
## Presentación

La capa de presentación proporciona una representación común de los datos transferidos entre los servicios de la capa de aplicación.

## Aplicación

La capa de aplicación proporciona los medios para la conectividad de extremo a extremo entre individuos de la red humana mediante redes de datos.

- **Aplicación:** define los protocolos de cada una de las aplicaciones que utilizamos para poder ser utilizadas en la red. Es donde los usuarios interactúan entre sí. El resto de capas existen para prestar servicios a esta capa. Para la gente que trabaja en programación (tiene que seguir unos estándares, reglas >>> protocolos).
- **Presentación:** responsable de como se presentan los datos al usuario y responsable de hacer que los datos sean legibles al usuario. Información enviada por esta capa desde un host sea entendida por la misma capa del otro host. Ejemplo: formato de archivos. Adaptar la información al protocolo que se esté usando.
- **Sesión:** establecer, administrar y terminar las **sesiones** entre dos hosts que se comunican. Administra el **intercambio de datos** y sincroniza el diálogo. Control de flujos de la misma sesión y como deben terminar correctamente.
- **Transporte:** establecer y mantener **conexión lógica extremo a extremo**. Define los servicios para **segmentar, transferir y rearmar los datos** para las comunicaciones entre los hosts. Paquetes tengan secuencias correctas y detección de errores. Control de flujo y de congestión. **Multiplexación** para las aplicaciones, diferentes puertos para cada aplicación y diferentes usuarios accediendo a un mismo puerto.
- **Red:** separa los datos en paquetes, determina la **ruta** que tomarán los datos, se encarga de definir el **direcccionamiento lógico**.
- **Enlace de Datos:** empaqueta los datos para trasmitirlos a través de la capa física, intercambiar tramas entre dispositivos en un medio común, acceso a los medios de transmisión y control de errores, define dirección física de los nodos. Esta capa depende de la topología y el medio utilizados.
- **Física:** dispositivo electrónico se encarga de **traducir o interpretar los 0y1 lógicos** en señales eléctricas, luminosas, etc. Su función es la de **codificar** las señales binarias y **transmitirlas** a través del medio. Tiene que ver con conectores, pines, corriente eléctrica, cableado, etc.



Recurso vídeo: Modelo de Referencia OSI

<https://www.youtube.com/watch?v=vfcPqnWYI1E&feature=youtu.be>

Pila de capas o niveles del modelo OSI (Open System Interconnection).

Si necesitas ampliar o conocer más sobre el modelo OSI te recomendamos el artículo de la wikipedia que trata sobre el modelo.

[http://es.wikipedia.org/wiki/Modelo\\_OSI](http://es.wikipedia.org/wiki/Modelo_OSI)

Es especialmente recomendable que dediques un tiempo al siguiente **vídeo** donde encontrarás una explicación bastante completa de todo el modelo OSI.

[http://www.youtube.com/watch?v=J4fyelWeq-Q&feature=player\\_embedded#!](http://www.youtube.com/watch?v=J4fyelWeq-Q&feature=player_embedded#!)

# Modelo de Capas TCP/IP.

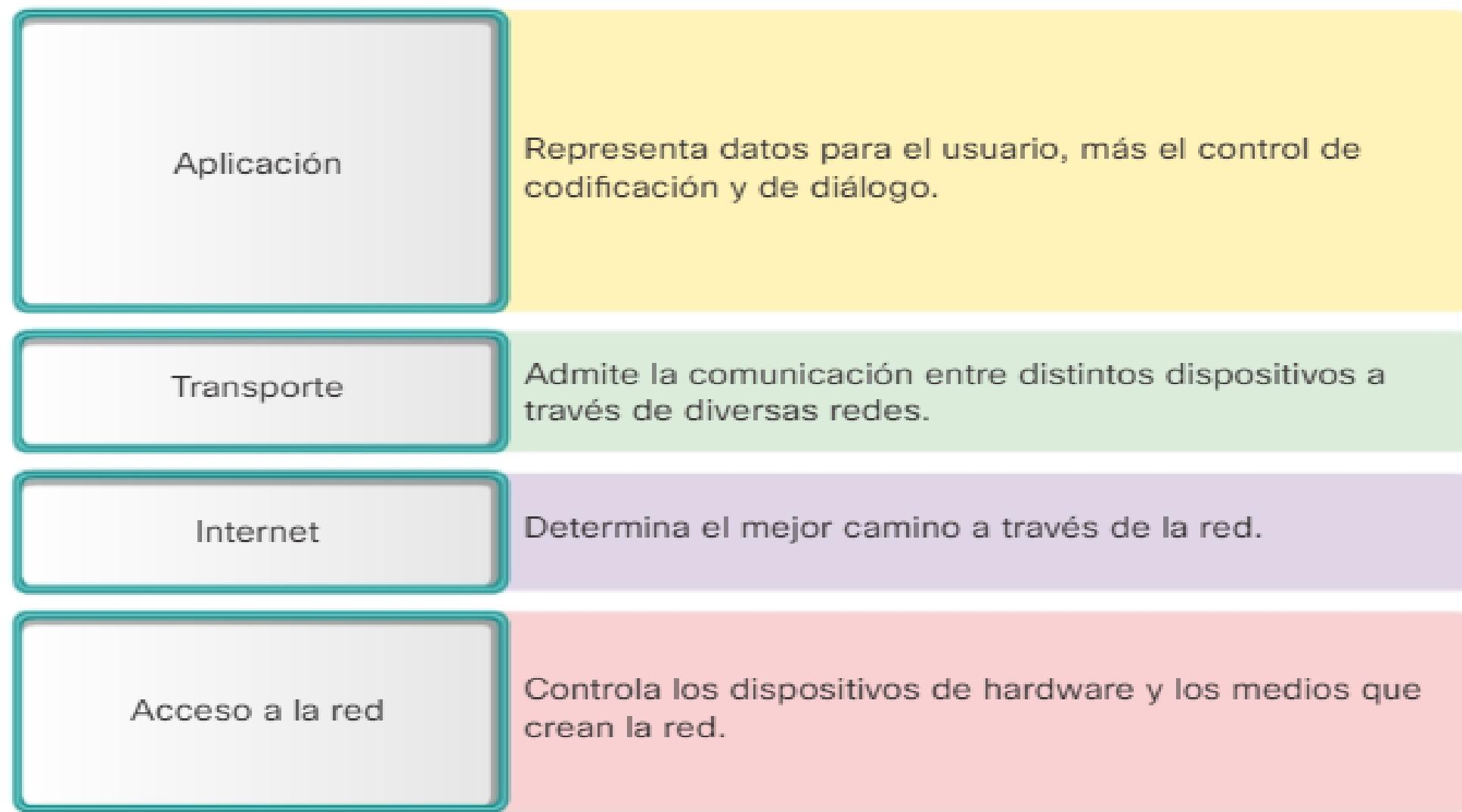
Cuando se habla de protocolos TCP/IP, realmente se suele estar **haciendo referencia a la arquitectura de red que incluye varios protocolos de red**, de entre los cuales dos de los más destacados son:

- El protocolo **TCP** (Protocolo de Control de Transmisión)
- El protocolo **IP** (Protocolo de Internet).

Considerar este modelo como una arquitectura en sí, siendo la más utilizada, ya que es la **base de las comunicaciones de Internet y de los sistemas operativos modernos**.

Cuando nos referimos a la arquitectura TCP/IP o modelo TCP/IP, nos estamos refiriendo a un **conjunto de reglas generales de diseño e implementación de protocolos de red, que permiten la comunicación de los ordenadores**.

Existen **protocolos para los diferentes tipos de servicios de red**.



- TCP/IP es un **estándar abierto**, no hay una compañía que 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 RFC** disponibles al público.
- Las RFC contienen las **especificaciones formales** de los protocolos de comunicación de datos y los recursos que describen el uso de los protocolos.

# La arquitectura TCP/IP está compuesta de cuatro capas o niveles que son:

Capa o nivel de acceso a la red, de enlace o también llamado de subred.	Se encarga del acceso al medio de transmisión, es asimilable a los niveles 1 y 2 del modelo OSI, y sólo especifica que deben usarse protocolos que permitan la conexión entre ordenadores de la red. Hay que tener en cuenta que esta arquitectura está pensada para conectar ordenadores diferentes en redes diferentes, por lo que las cuestiones de nivel físico no se tratan, y se dejan lo suficientemente abiertas para que se puedan utilizar cualquier estándar de conexión. Permite y define el uso de direcciones físicas utilizando las direcciones MAC.
Capa o nivel de red también llamada de Internet.	Al igual que la capa de red del modelo OSI, esta capa se encarga de estructurar la información en paquetes, determina la ruta que tomarán los paquetes y define el direccionamiento. En esta arquitectura los paquetes pueden viajar hasta el destino de forma independiente, pudiendo atravesar redes diferentes y llegar desordenados, sin que la ordenación de los paquetes sea responsabilidad de esta capa, por tanto tampoco se encarga de los errores. El protocolo más significativo de esta capa es el protocolo IP, y entre sus funciones está la de dar una dirección lógica a todos los nodos de la red.
Capa o nivel de transporte.	Es igual al nivel de transporte del modelo OSI. Se encarga de que los paquetes de datos tengan una secuencia adecuada y de controlar los errores. Los protocolos más importantes de esta capa son: TCP y UDP. El protocolo TCP es un protocolo orientado a conexión y fiable, y el protocolo UDP es un protocolo no orientado a conexión y no fiable.
Capa o nivel de Aplicación.	Esta capa englobaría conceptos de las capas de sesión, presentación y aplicación del modelo OSI. Incluye todos los protocolos de alto nivel relacionados con las aplicaciones que se utilizan en Internet.

Debes leer el artículo del Modelo TCP/IP de la wikipedia, y prestar especial atención al gráfico donde se representa la encapsulación de una aplicación de datos a través del modelo, ya que te será necesario para poder entender los siguientes puntos de la unidad.

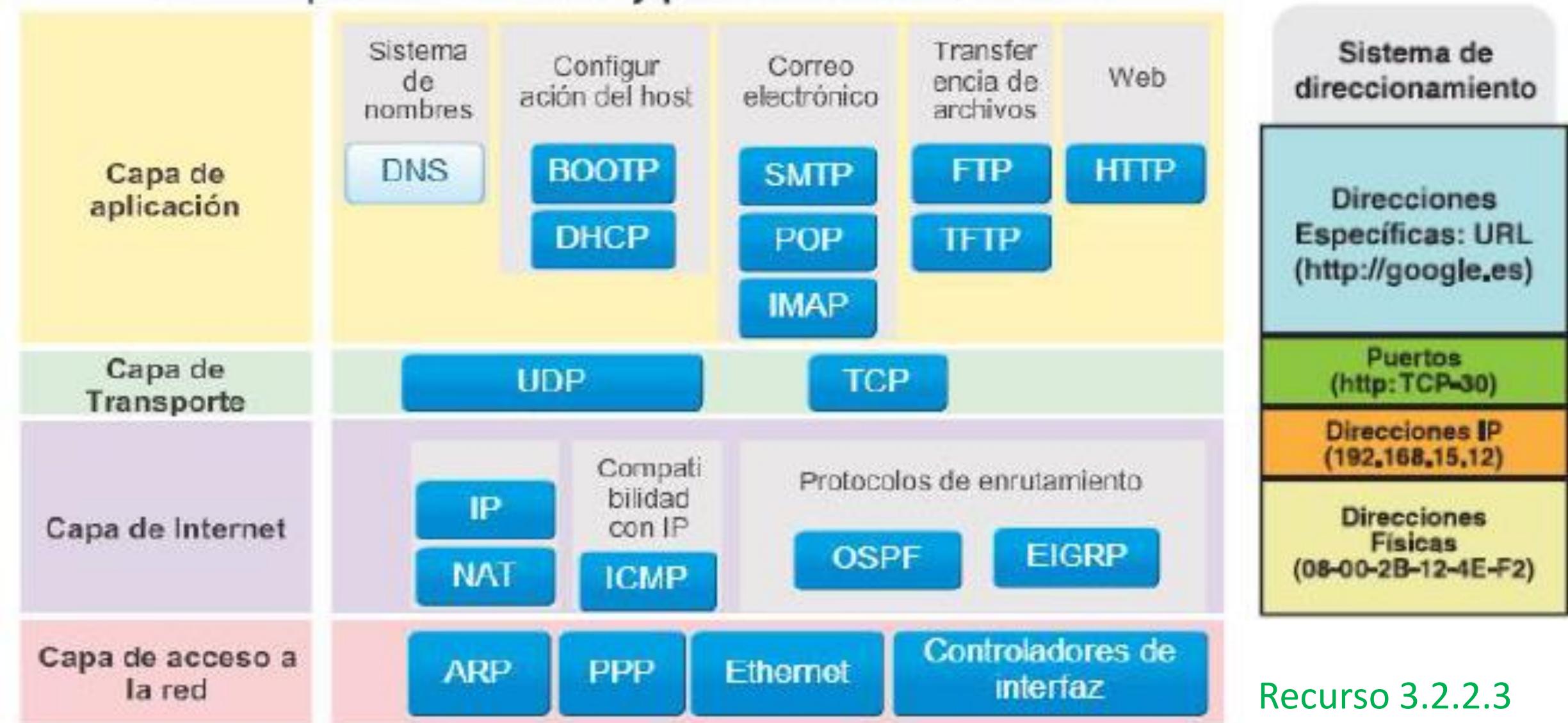
[http://es.wikipedia.org/wiki/Modelo\\_TCP/IP](http://es.wikipedia.org/wiki/Modelo_TCP/IP)

- Capa 4 o **capa de aplicación**: aplicación, asimilable a las capas: 5 (sesión), 6 (presentación) y 7 (aplicación), del modelo OSI. La capa de aplicación debía incluir los detalles de las capas de sesión y presentación OSI.
- Capa 3 o **capa de transporte**: transporte, asimilable a la capa 4 (transporte) del modelo OSI.
- Capa 2 o **capa de internet**: Internet, asimilable a la capa 3 (red) del modelo OSI.
- Capa 1 o **capa de acceso al medio**: acceso al medio, asimilable a la capa 2 (enlace de datos) y a la capa 1 (física) del modelo OSI.

**Recurso. Mostrar vídeo:** El Modelo TCP/IP

<https://www.youtube.com/watch?v=JQDCL17sARA&feature=youtu.be>

## Suite de protocolos TCP/IP y proceso de comunicación

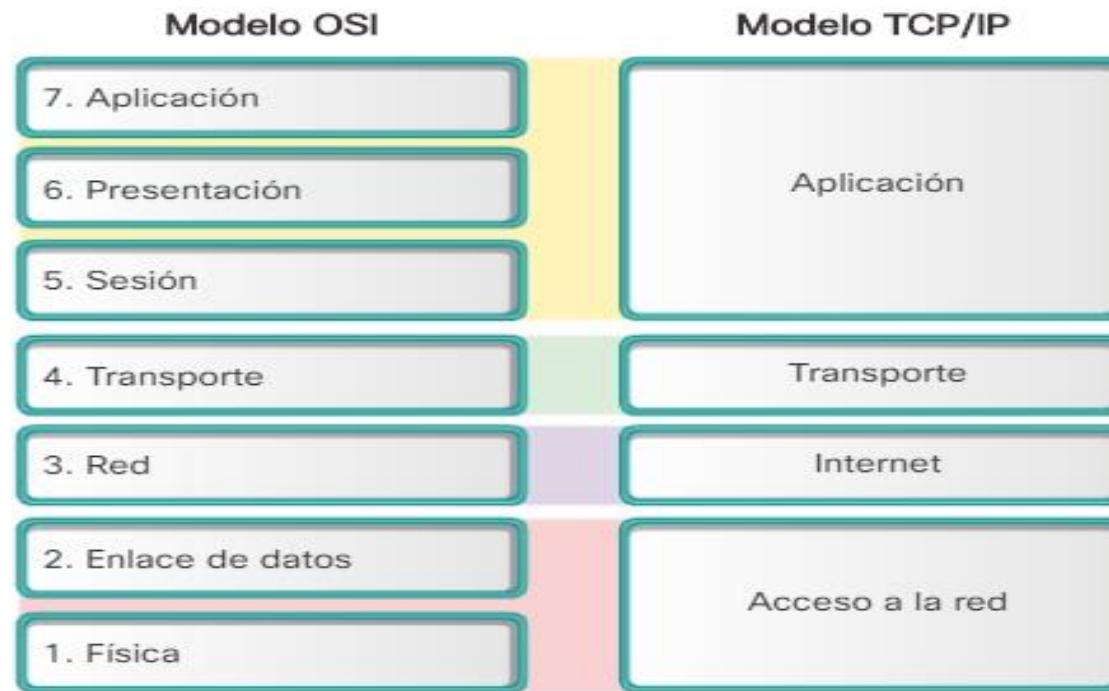


Recurso 3.2.2.3

Recurso vídeo: Símil Arquitectura TCP/IP

<https://www.youtube.com/watch?v=WnvSsQQ0z5Y&feature=youtu.be>

Una comparativa de esta arquitectura con el modelo OSI podemos verla en el siguiente gráfico.



La arquitectura TCP/IP se estructura en **capas jerarquizadas** y es el utilizado en **Internet**, por lo que en algunos casos se denomina **Familia de Protocolos de Internet** refiriéndose a está arquitectura cuando trabaja en Internet.

En algunos casos se **divide la capa de acceso a la red**, en capa de **hardware** o física y **enlace de datos**, con lo que la arquitectura tendría **cinco niveles** en vez de cuatro. Esto suele hacerse en referencia al modelo OSI. En realidad esto se puede hacer y no cambiaría la estructura de la arquitectura.

## Encapsulación de Datos

Para transmitir los datos, el mejor método es **dividir** los datos en partes más pequeñas y manejables para enviarlas por la red. La división de, por ejemplo, un stream de datos en partes más pequeñas se denomina **segmentación**.

La segmentación de mensajes tiene dos **beneficios** principales:

- Al enviar partes individuales más pequeñas del origen al destino, se pueden **intercalar** muchas **conversaciones** diversas en la red >> **multiplexación**.
- puede aumentar la **confiabilidad** de las comunicaciones de red. No es necesario que las partes separadas de cada mensaje sigan el mismo recorrido a través de la red desde el origen hasta el destino. Si una ruta en particular se satura con el tráfico de datos, o falla, las **partes individuales** del mensaje aún **pueden direccionarse** hacia el destino mediante los **recorridos alternativos**.
- si parte del mensaje no logra llegar al destino, solo se deben **retransmitir las partes faltantes**.

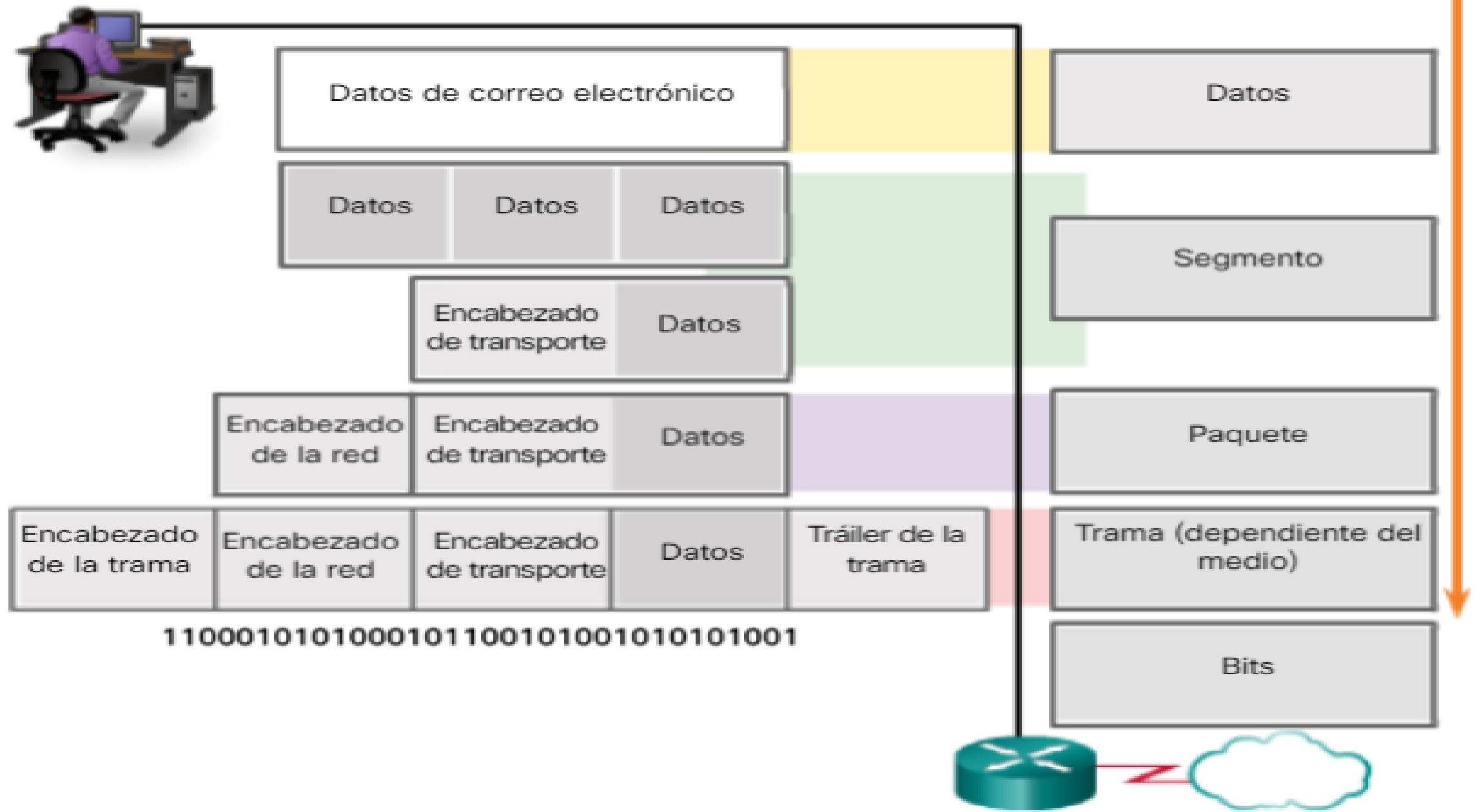
### Mostrar Recurso 3.3.1.1

La **desventaja**:

- el nivel de **complejidad** que se agrega al proceso.

*Ejemplo: Supongamos que tuviera que enviar una carta de 100 páginas, pero en cada sobre solo cabe una. El proceso de escribir la dirección, etiquetar, enviar, recibir y abrir los 100 sobres requeriría mucho tiempo tanto para el emisor como para el destinatario.*

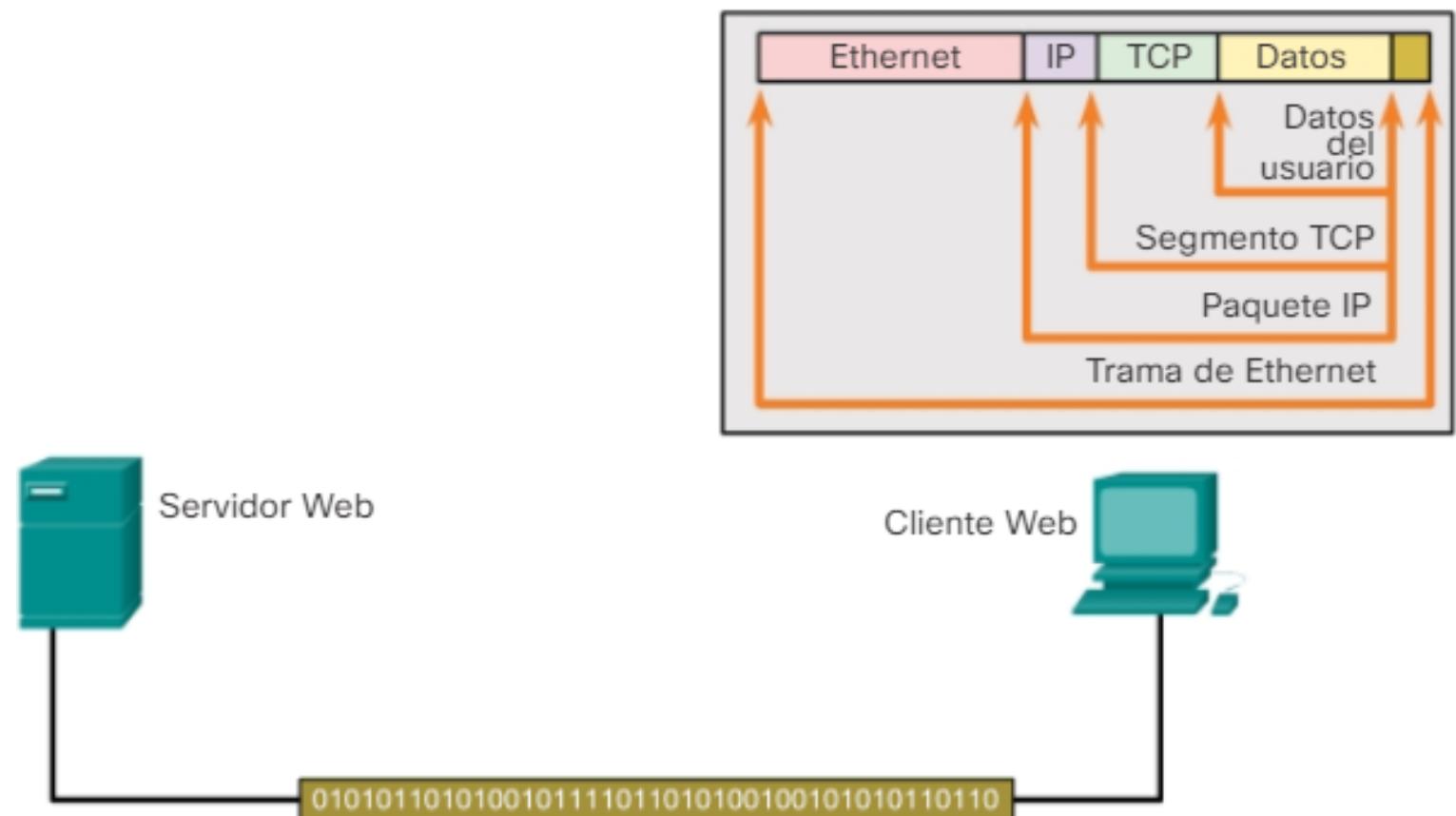
Paso por el stack.



# Desencapsulación

El proceso se invierte en el host receptor, y se conoce como “**desencapsulación**”. Es el proceso que utilizan los dispositivos receptores para eliminar uno o más de los encabezados de protocolo. Los datos se desencapsulan mientras suben por la pila (stack) hacia la aplicación del usuario final.

[Mostrar Recurso 3.3.1.3](#)



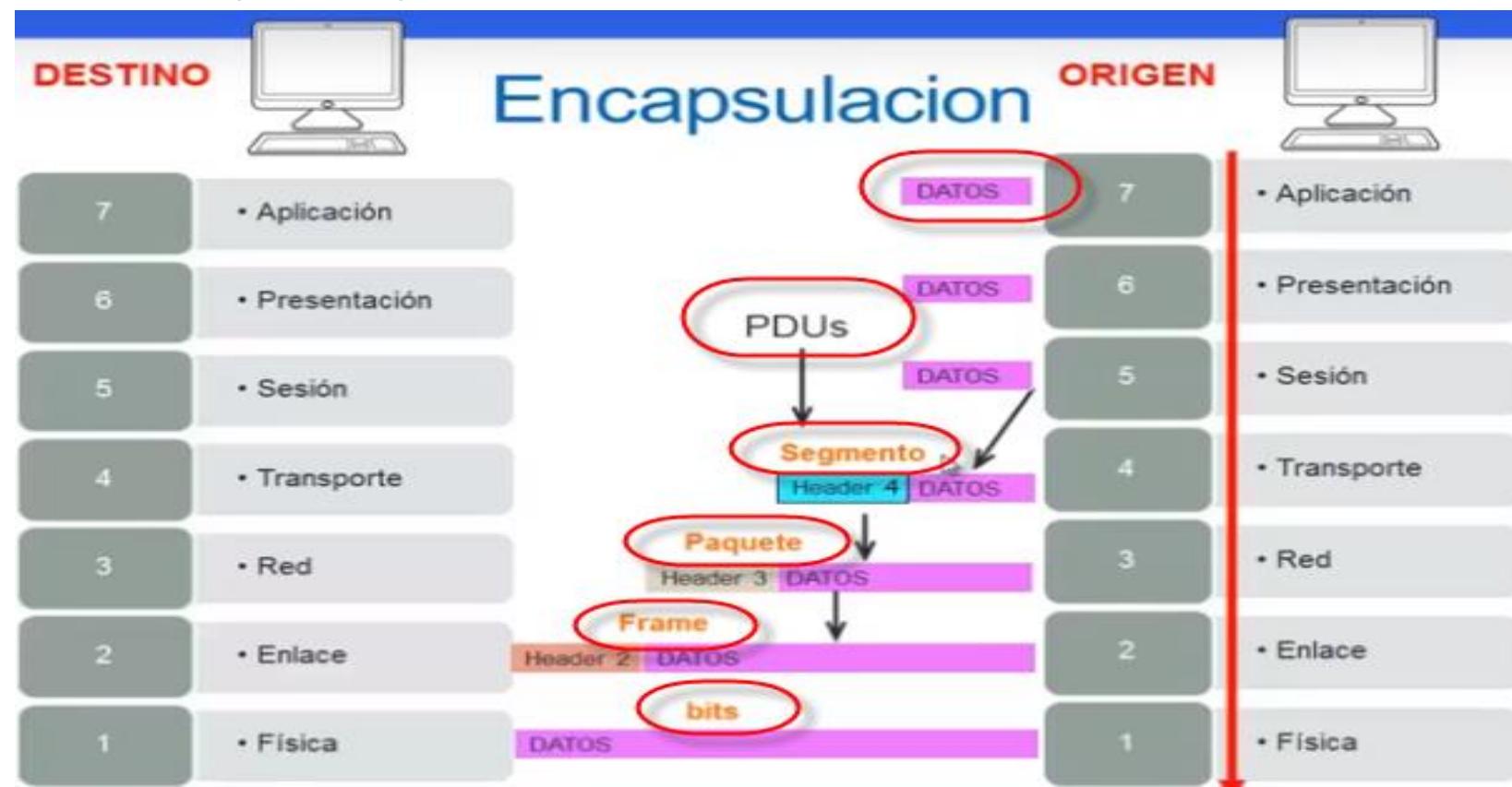
## Unidades de datos del protocolo (PDU).

Mientras los **datos** de la aplicación **bajan por la pila del protocolo** y se transmiten por los medios de la red, los **protocolos le agregan información en cada nivel**. Esto comúnmente se conoce como proceso de **encapsulación**.

La forma que adopta una porción de datos en cualquier capa se denomina **PDU** (Unidad de Datos del Protocolo).

En cada etapa del proceso, la PDU tiene un nombre distinto para reflejar sus nuevas funciones:

- **Datos**: término general que se utiliza en la capa de **aplicación**.
- **Segmento**: capa de **transporte**.
- **Paquete**: capa de **red**.
- **Trama**: capa de **enlace de datos**.
- **Bits**: capa física



## Capa1. Capa Física(1).

La arquitectura TCP/IP en su estandarización **original no se preocupaba demasiado del nivel físico** en sí, de hecho, en un principio sólo se preocupó de estandarizar los protocolos relacionados con el enlace de datos, de ahí el nombre de este nivel.

Posteriormente con el **auge de las redes de todo tipo**, se vio que los estándares que ya existían desde un punto de vista **físico**, cada vez se tenían que tener más en cuenta, y por esto algunos autores, desarrolladores y diseñadores consideran que la arquitectura TCP/IP realmente consta de cinco capas, siendo la primera la capa **física** o de hardware y la segunda la de enlace de datos, tal y como recomienda el modelo OSI.

En el emisor, la función de la **capa de enlace de datos** es:

- preparar los datos para la transmisión y controlar la forma en que estos acceden a los medios físicos.

La **capa física** controla:

- cómo se transmiten los datos a los medios físicos mediante la **codificación en señales de los dígitos binarios** que representan los datos.

Así pues, la **principal función** de este nivel es:

- **convertir la información** suministrada por el nivel de red, en **señales** que puedan ser **transmitidas por el medio físico**.
- **función inversa** es convertir las señales que llegan por el medio físico en paquetes de información manejables por el nivel de red.

En este nivel se deben tener en cuenta **cuestiones relacionadas con las conexiones físicas**, que en las **redes locales vienen definidas por el estándar Ethernet**.

Este estándar define:

- las **características de cableado** y **señalización** de nivel físico
- los **formatos** de las tramas de datos del nivel de enlace de datos.

Ethernet es la base para el **estándar IEEE 802.3**, que es un estándar internacional.

Artículo sobre Ethernet y su evolución al estándar IEEE 802.3.

<http://es.wikipedia.org/wiki/Ethernet>

# Tarjetas de interfaz de red (NIC).

Conectan un dispositivo a la red.

- Las NIC Ethernet se utilizan para las conexiones por **cable**
- Las NIC de red de área local inalámbrica (WLAN) se utilizan para las conexiones **inalámbricas**.

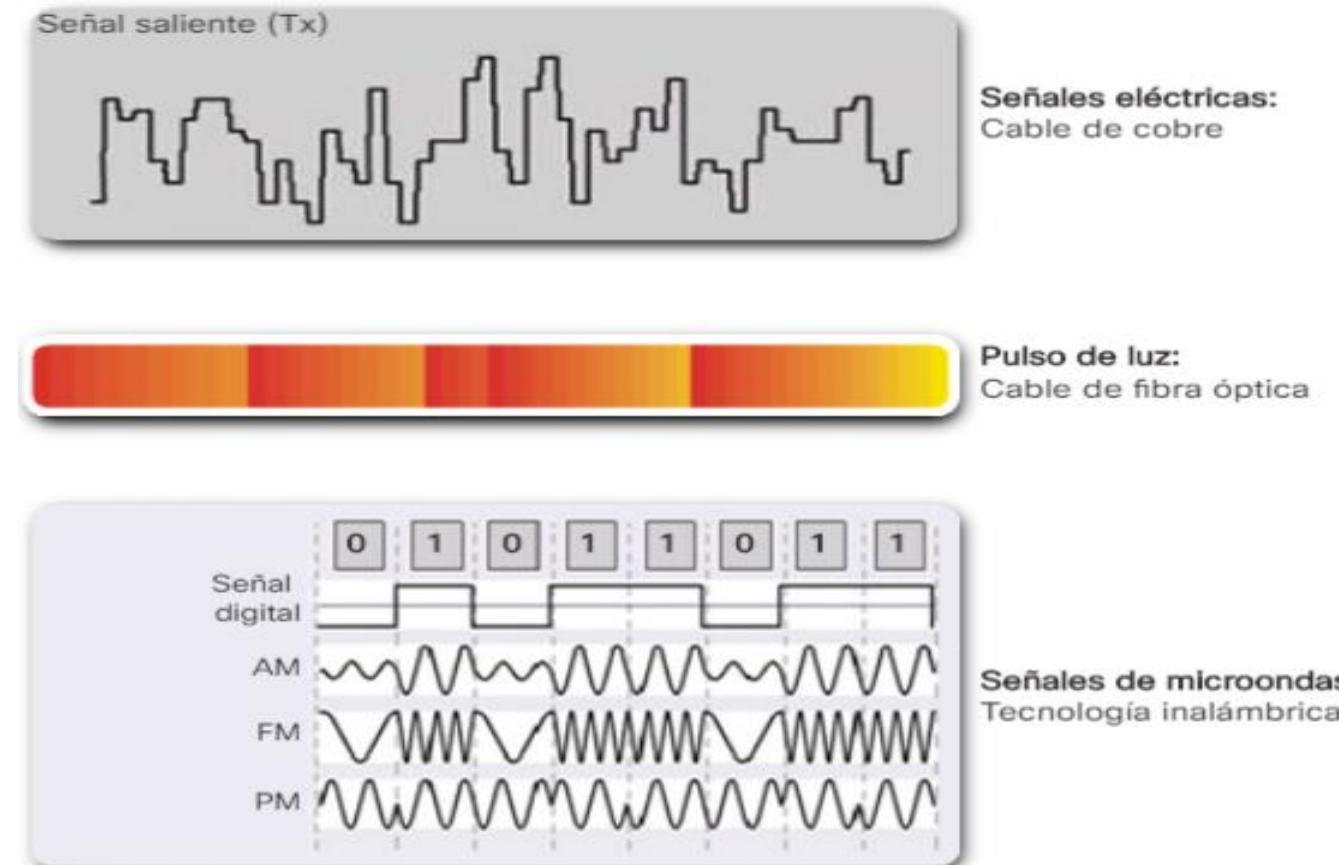
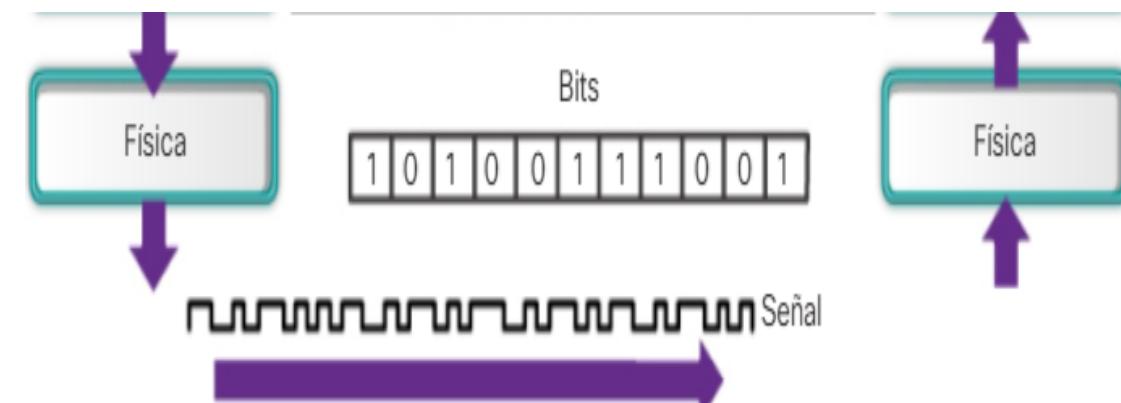


Existen tres formatos básicos de **medios de red**.

La capa física produce la representación y las agrupaciones de bits para cada tipo de medio de la siguiente manera:

- Cable de **cobre**: las señales son patrones de pulsos eléctricos.
  - Cable de **fibra óptica**: las señales son patrones de luz.
  - Conexión **inalámbrica**: las señales son patrones de transmisiones de **microondas**.

Para habilitar la **interoperabilidad** de la capa física, los organismos de **estandarización** rigen todos los aspectos de estas funciones.



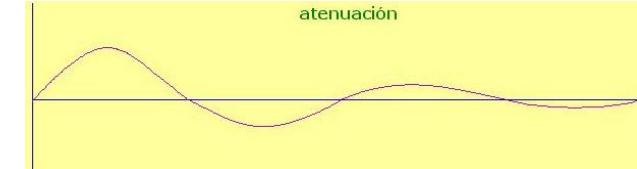
# Características de los medios de cobre

## Ventajas:

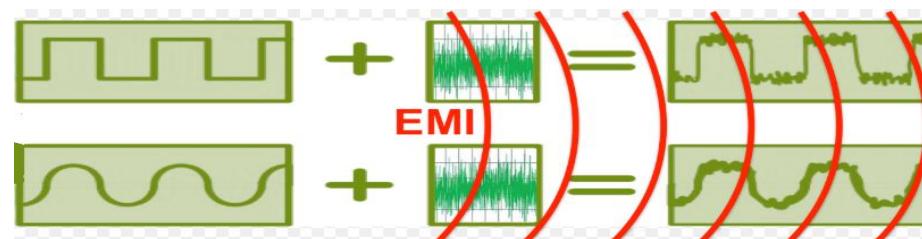
- Económicos
- Fáciles de instalar
- Baja resistencia a la corriente eléctrica.

## Desventajas:

Están limitados por la **distancia** y la **interferencia** de señales.



- **Atenuación**: los datos se **transmiten** en cables de cobre **como impulsos eléctricos**. Cuanto mayor sea la distancia que recorre la señal, más se deteriora.
- **Crosstalk (XT) o diafonía**: perturbación electromagnética producida en un canal de comunicación por el acoplamiento de este con otro u otros vecinos.
- **Interferencia electromagnética (EMI)** o **interferencia de radiofrecuencia (RFI)**: las señales de EMI y RFI pueden distorsionar y dañar las señales de datos que transportan los medios de cobre. Las posibles fuentes de EMI y RFI incluyen las ondas de radio y dispositivos electromagnéticos como las luces fluorescentes o los motores eléctricos

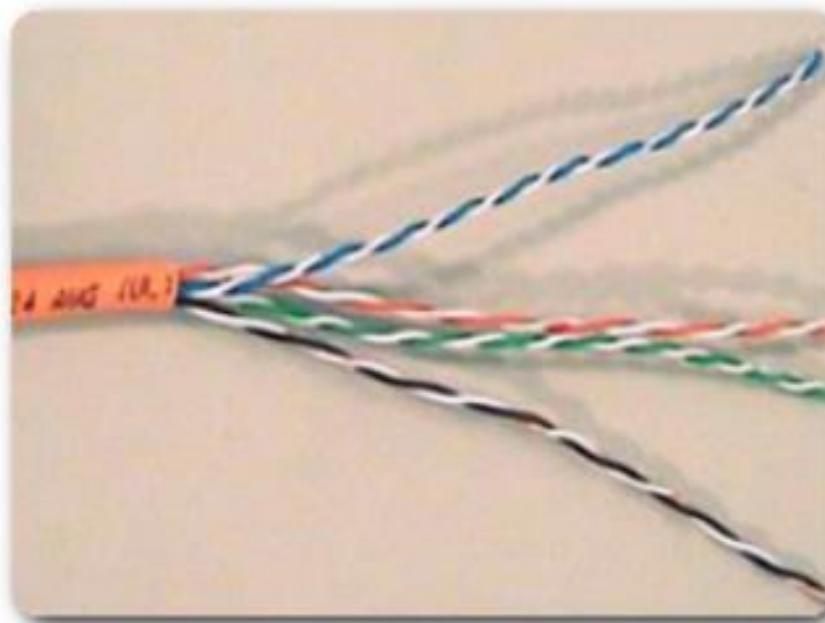


Deben seguir limitaciones de distancia estrictas según lo especifican estándares que los rigen.

[Mostrar Recurso 4.2.1.1](#)

Existen **tres** tipos principales de medios de **cobre** que se utilizan en las redes:

- Par trenzado **no blindado (UTP)**
- Par trenzado **blindado (STP)**
- **Coaxial**



Cable de par trenzado no blindado (UTP)



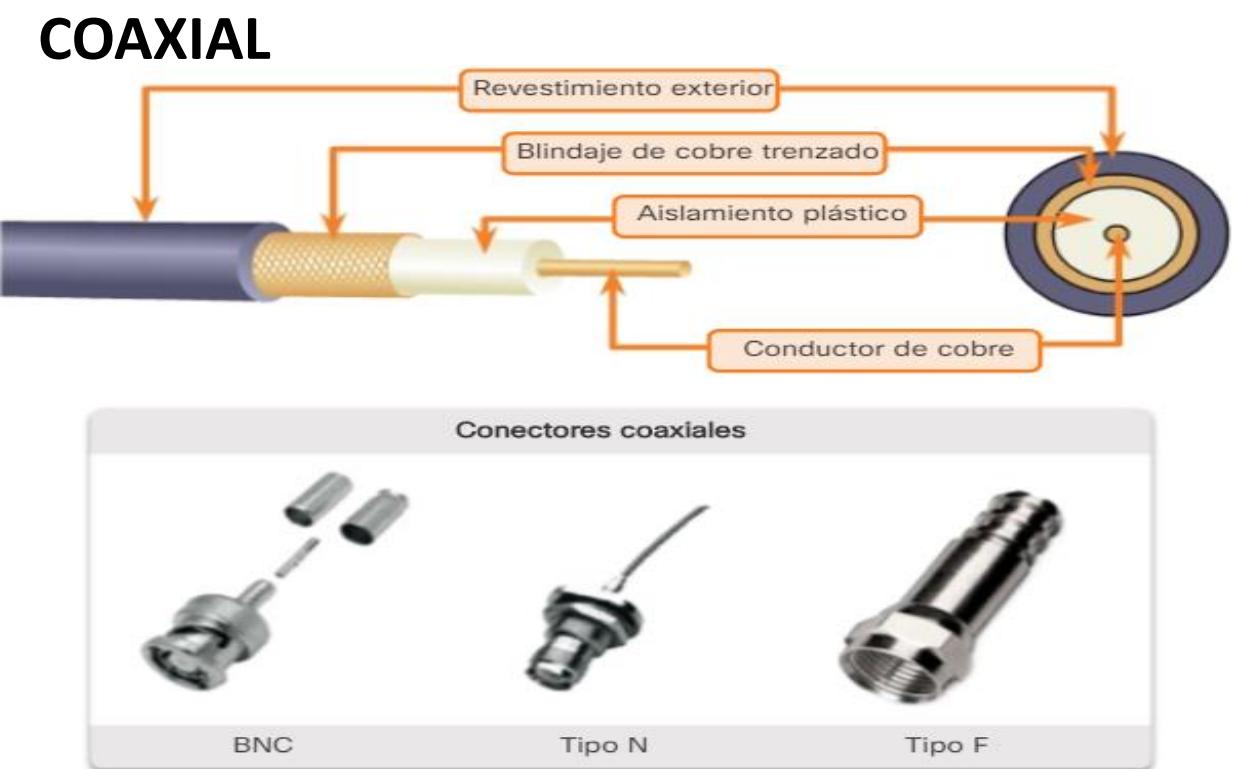
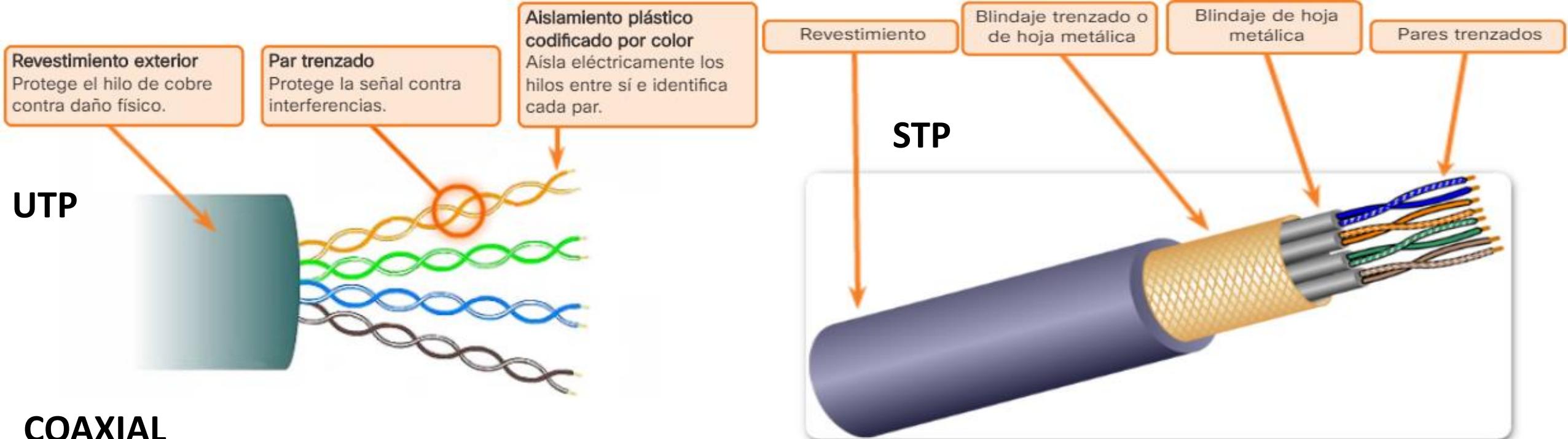
Cable de par trenzado blindado (STP)

Se utilizan para **interconectar los nodos** en una LAN y los **dispositivos de infraestructura**, como switches, routers y puntos de acceso inalámbrico.

Cada tipo de conexión y sus dispositivos complementarios tienen requisitos de cableado estipulados por los **estándares de la capa física**.



Cable coaxial



El cable UTP **reemplazó** al cable coaxial en las instalaciones de Ethernet modernas. El cable coaxial se adaptó principalmente para:

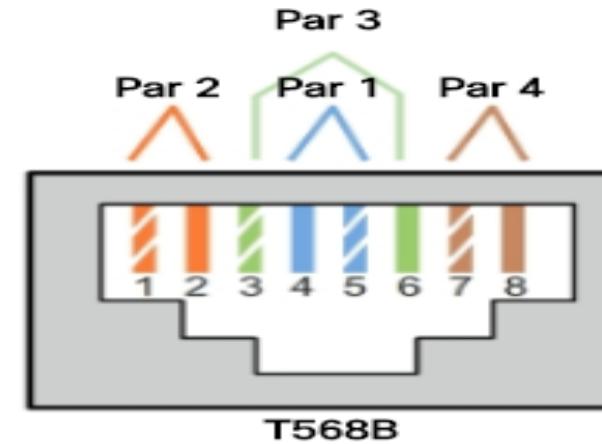
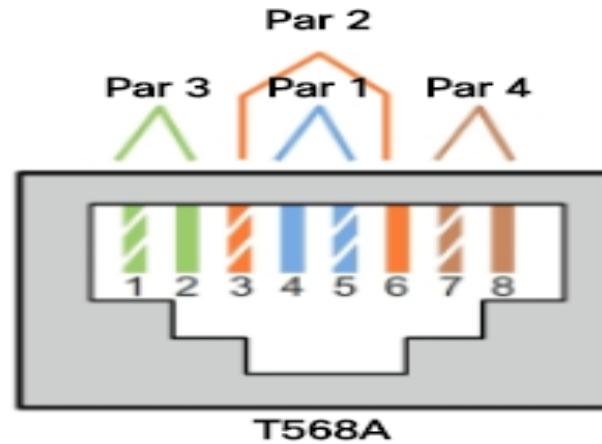
- Instalaciones de **Internet por cable**: sistemas bidireccionales para proporcionar a los clientes conectividad a Internet. Las partes de cable coaxial y los elementos de amplificación compatibles se reemplazan con cables de fibra óptica. Sin embargo, la conexión final hacia la ubicación del cliente y el cableado dentro de sus instalaciones aún sigue siendo de cable coaxial. Este uso combinado de fibra y coaxial se denomina fibra coaxial híbrida (**HFC**).

# Tipos de cables UTP

Es posible que los hilos individuales del cable deben conectarse en diferente orden para distintos grupos de pines en los conectores RJ-45.

Principales tipos de cables que se obtienen al utilizar convenciones específicas de cableado:

- **Cable directo de Ethernet:** el tipo **más común** de cable de red. Para interconectar un host con un switch y un switch con un router.
- **Cable cruzado Ethernet:** cable poco común utilizado para interconectar **dispositivos similares**. Para conectar un switch a un switch, un host a un host o un router a un router.



Tipo de cable	Estándar	Capa de aplicación
Cable directo de Ethernet	Ambos extremos son T568A o T568B.	Conecta un host de red a un dispositivo de red, como un switch o un hub.
Cruzado Ethernet	Un extremo es T568A, el otro extremo es T568B.	<ul style="list-style-type: none"><li>• Conecta dos hosts de red.</li><li>• Conecta dos dispositivos de red intermediarios (un switch a un switch, o un router a un router).</li></ul>



# Propiedades del cableado de fibra óptica

Permite la transmisión de datos en:

- **distancias más extensas**
- **anchos de banda** (velocidades de datos) **mayores** que cualquier otro medio de red
- transmitir señales con **menos atenuación**
- totalmente **inmune a las EMI y RFI**
- **inmune a la diafonía**

*El ancho de banda es la capacidad de un medio para transportar datos. El ancho de banda digital mide la cantidad de datos que pueden fluir desde un lugar hasta otro en un período determinado. El ancho de banda generalmente se mide en kilobits por segundo (kb/s) o megabits por segundo (Mb/s).*

La fibra óptica es un **hilo flexible**, extremadamente **delgado** y **transparente** de **vidrio muy puro** (sílice), no mucho más grueso que un cabello humano. En la fibra, los **bits se codifican en forma de impulsos de luz**. El cable de fibra óptica actúa como una guía de ondas o una “tubería de luz” para transmitir la luz entre los dos extremos con una pérdida mínima de la señal.



La fibra consta de dos tipos de vidrio y de un blindaje externo de protección.

- **Núcleo:** consta de **vidrio puro** y es la parte de la fibra por la que se **transporta la luz**.
- **Cubierta:** el vidrio que **rodea al núcleo** y actúa como **espejo**. Los pulsos de luz se propagan por el núcleo mientras la cubierta los refleja. Esto ayuda a contener los pulsos de luz en el núcleo de la fibra, conocido como "**reflexión interna total**".
- **Revestimiento:** generalmente, es un revestimiento de PVC que **protege el núcleo y la cubierta**. También puede incluir material de refuerzo y un recubrimiento de protección cuyo objetivo es proteger el vidrio contra ratones y humedad.

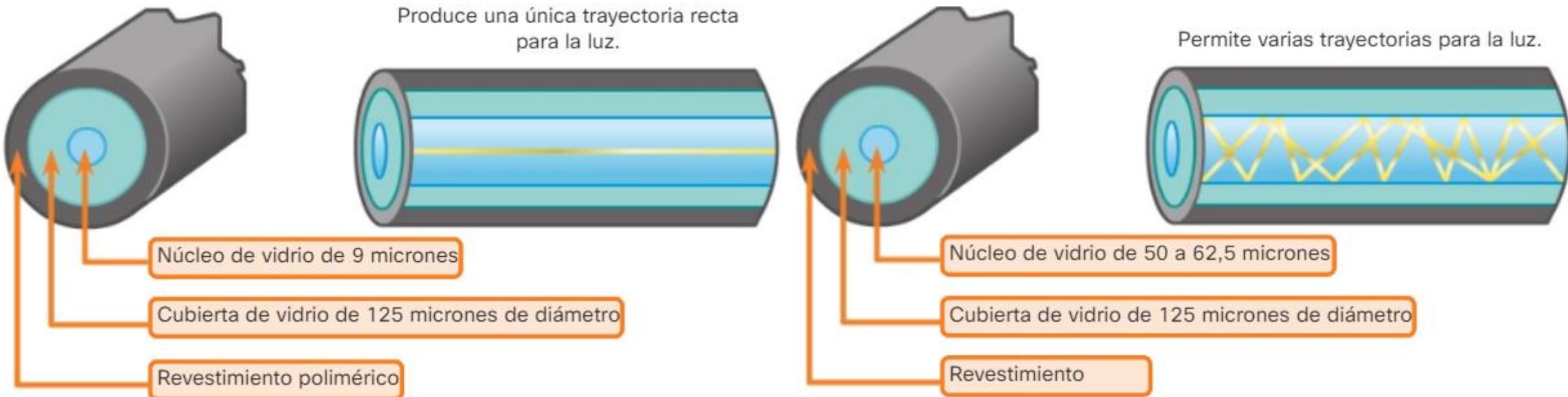


Los **pulsos de luz** que representan los datos transmitidos en forma de bits en los medios son **generados** por uno de los siguientes:

- **Láseres**
- **Diodos emisores de luz (LED)**

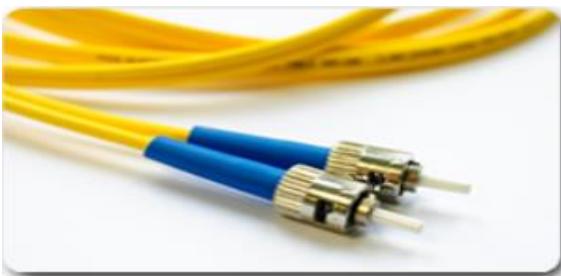
Los cables de fibra óptica pueden clasificarse en **dos tipos**:

- Fibra óptica **monomodo** (SMF): consta de un **núcleo muy pequeño** y emplea tecnología láser para enviar un **único haz de luz**. Se usa mucho en situaciones de **larga distancia** que abarcan cientos de kilómetros, como aplicaciones de TV por cable y telefonía de larga distancia.
- Fibra óptica **multimodo** (MMF): consta de un **núcleo más grande** y utiliza emisores LED para enviar pulsos de luz (más baratos). Específicamente, la **luz de un LED ingresa a la fibra multimodo en diferentes ángulos**, mayor **dispersión**. Se usa mucho en las **redes LAN**, debido a que se puede alimentar mediante LED de **bajo costo**. Proporciona un **ancho de banda de hasta 10 Gb/s** a través de longitudes de enlace de hasta 500m.



Los tres **conectores** de red de fibra óptica más populares son los siguientes:

- **Punta recta (ST)**: conectores antiguos de estilo bayoneta, ampliamente utilizados con la fibra óptica **multimodo**.
- **Conector suscriptor (SC)**: “conector cuadrado” o “conector estándar”. Es un conector LAN y WAN ampliamente adoptado que utiliza un **mecanismo de inserción/extracción** para asegurar la inserción correcta. Se utiliza con la fibra óptica **multimodo y monomodo**.
- **Conector Lucent (LC)**: conector “pequeño” o “local”, gran popularidad debido a su **tamaño reducido**. Se utiliza con la fibra óptica **monomodo** y también es compatible con la fibra óptica **multimodo**.



Conectores ST



Conectores SC



Conector LC



Conectores LC multimodo dúplex

## GBICs y SFP Ethernet

Gigabit Interface Converter  
GBIC



Small Form Factor Pluggables  
SFP



# Capa1. Capa de Enlace de Datos(2).

La capa de acceso a la red de TCP/IP equivale a las siguientes capas del modelo OSI:

- **Enlace de datos** (capa 2)
- **Física** (capa 1)

La capa de enlace de datos realiza **los siguientes servicios básicos**:

- Acepta paquetes de la capa 3 y los empaqueta en unidades de datos denominadas “tramas”.
- Permite que las **capas superiores accedan** a los medios.
- Controla el **acceso al medio** y realiza la **detección de errores**: especifican la encapsulación de un paquete en una trama y las **técnicas para colocar y sacar el paquete encapsulado de cada medio**.
- Regula como se da **formato a una trama**.

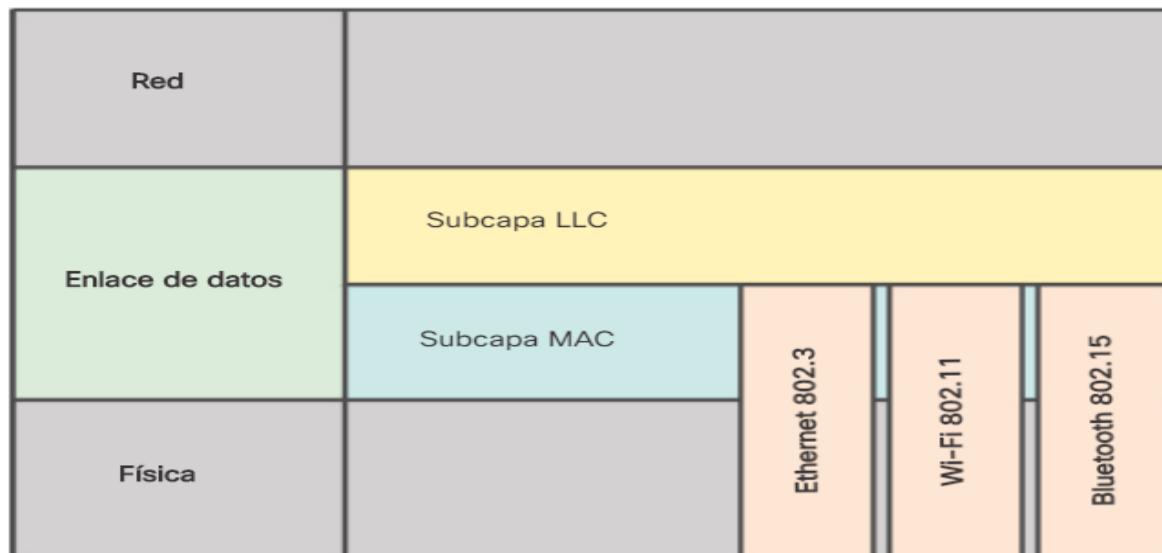
Los protocolos de capa de enlace de datos regulan cómo se da formato a una trama para utilizarla en diferentes medios.

Diversos protocolos pueden estar en uso para medios diferentes.



La capa de enlace de datos se **divide en dos subcapas**:

- **Control de enlace lógico (LLC)**
  - define los **procesos** de software que dan servicios a los protocolos de capa de red
  - **coloca en la trama información** que identifica qué protocolo de capa de red se utiliza. Permite que varios protocolos de la capa 3, tales como IPv4 e IPv6, utilicen la misma interfaz y los mismos medios de red.
- **Control de acceso al medio (MAC)**:
  - define los procesos de **acceso al medio que realiza el hardware**.
  - proporciona **direcccionamiento de la capa de enlace de datos (MAC)**
  - delimitación de los datos de acuerdo con los requisitos de señalización física del **medio** y con el tipo de **protocolo (Ethernet, WiFi, Bluetooth)** de capa de enlace de datos en uso.



El direccionamiento físico viene de la subcapa del nivel de enlace de datos, **Control de Acceso al Medio (MAC)**, se utilizan para definir lo que se conoce como direcciones MAC.

Las **dirección MAC** es un identificador de 48 bits, que suele representarse en forma de números Hexadecimales:

- en un formato de **6 bloques**
- de **dos números hexadecimales**
- divididos por **dos puntos**

El formato es el siguiente: **FF:FF:FF:FF:FF:FF**

*NOTA: para representar un número hexadecimal necesitamos 4bits*

24 bits más significativos (izquierda) determinan el **fabricante**, se conoce como **Identificador Único de Organización**  
24 bits menos significativos (derecha) identifican **una interfaz concreta**. Ninguna tarjeta tiene misma dirección MAC

**Actividad: Averigua por comandos o gráficamente la MAC de tú ordenador(móvil)**

**Averigua el Fabricante (<https://www.macvendorlookup.com> /// <https://hwaddress.com>)**

Para conocer la dirección MAC en diferentes sistemas operativos puede consultar el enlace:

**[http://es.wikipedia.org/wiki/Direcci%C3%B3n\\_MAC](http://es.wikipedia.org/wiki/Direcci%C3%B3n_MAC)**

- **getmac /fo table /nh /v**
- **ipconfig /all**

## Formato de la unidad de información de este nivel (PDU).

En este nivel la PDU se llama **TRAMA**, y tiene un formato determinado:

- Datos que recibimos de las capas superior

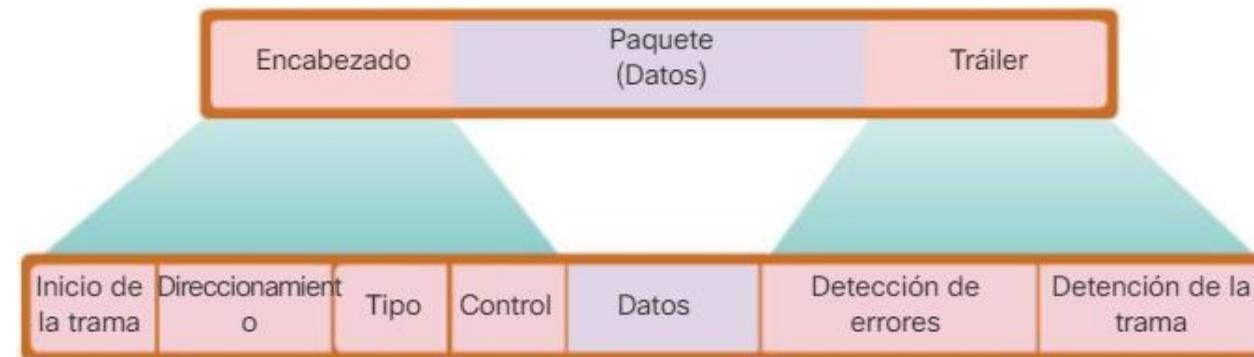
- Cabecera que agrega la capa de enlace:

- con las direcciones MAC origen y destino
- el tipo de trama Ethernet que se utiliza
- cola donde se agrega información para el control de errores



Tipos de **campos** de trama genéricos :

- Indicadores de **comienzo y de detención de la trama**: identificar inicio y final de la trama.
- **Direccionamiento**: identificar los nodos de origen y destino.
- **Tipo**: el LLC utiliza este campo para identificar el protocolo de capa 3.
- **Control**: identifica servicios especiales de control del flujo.
- **Datos**: incluye el contenido de la trama (es decir, los datos de niveles superiores).
- **Detección de errores**: para formar el tráiler, se utilizan para la detección de errores.



En este nivel hay un protocolo relacionado con el direccionamiento físico:

**ARP (protocolo de resolución de direcciones)**: trabaja **nivel de enlace de datos** y se encarga de **encontrar la dirección física (MAC) que tiene relación con la dirección lógica (dirección IP)**, es decir, traducir direcciones lógicas (IP) a direcciones físicas (MAC).

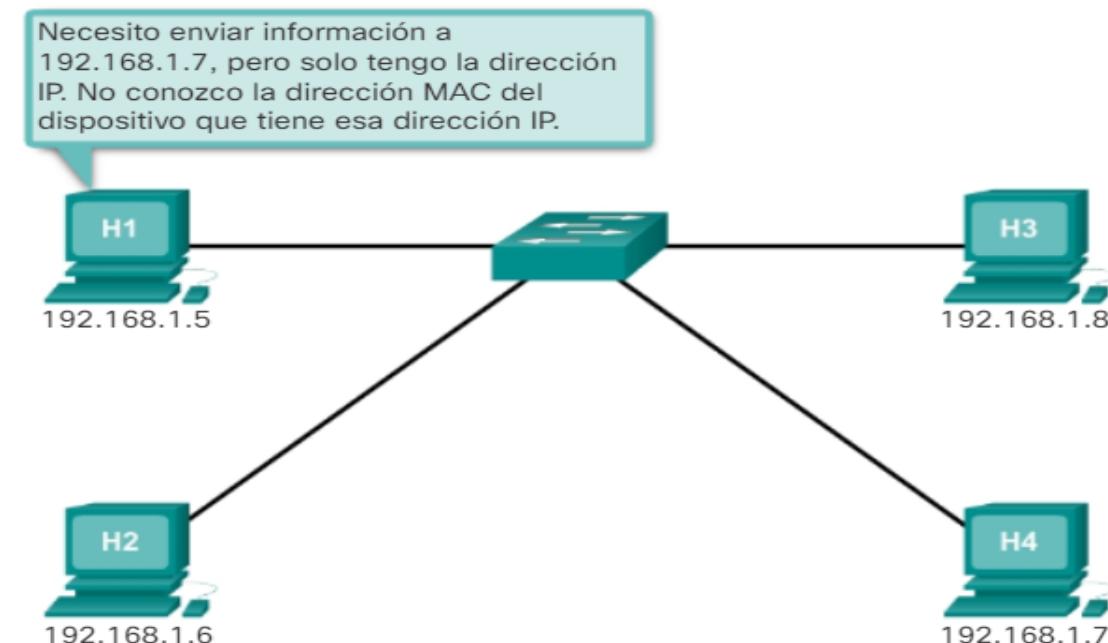
Cada nodo de una red IP tiene tanto una **dirección MAC como una dirección IP**. Para enviar datos, el nodo debe **utilizar ambas direcciones**. El nodo debe utilizar sus propias direcciones MAC e IP en los campos de **origen** y debe proporcionar una dirección MAC y una dirección IP para el **destino**.

El protocolo ARP se basa en determinados tipos de mensajes Ethernet de **broadcast** y **unicast**, denominados “**solicitudes ARP**” y “**respuestas ARP**”.

El protocolo ARP ofrece **dos funciones** básicas:

- **Resolución** de direcciones IPv4 a direcciones MAC
- Mantenimiento de una **tabla de las asignaciones**

**Mostrar Recurso 5.2.1.2**



Para cada dispositivo, un **temporizador de caché ARP** elimina las entradas ARP que no se hayan utilizado durante un período de tiempo especificado. Los tiempos difieren dependiendo del dispositivo y su sistema operativo. También pueden utilizarse **comandos** para eliminar manualmente todas o algunas de las entradas de la tabla ARP. Después de eliminar una entrada, el proceso para enviar una solicitud de ARP y recibir una respuesta de ARP debe ocurrir nuevamente para ingresar la asignación en la tabla ARP.

[Actividad 5.2.1.8 Observing ARP with the Windows CLI and Wireshark](#)

[Actividad 3.3.3.4 Using Wireshark to View Network Traffic](#)

[Actividad 5.1.4.3 Using Wireshark to Examine Ethernet Frames](#)

## Capa2 o Nivel de Internet.

La capa de red (capa3) en el modelo OSI, proporciona servicios que permiten que los **dispositivos finales intercambien datos a través de la red**.

El nivel de red del modelo TCP/IP se considera el **nivel de la arquitectura más importante**, ya que permite que las **estaciones envíen información a la red en forma de paquetes**.

Estos paquetes **vianjan** por la red:

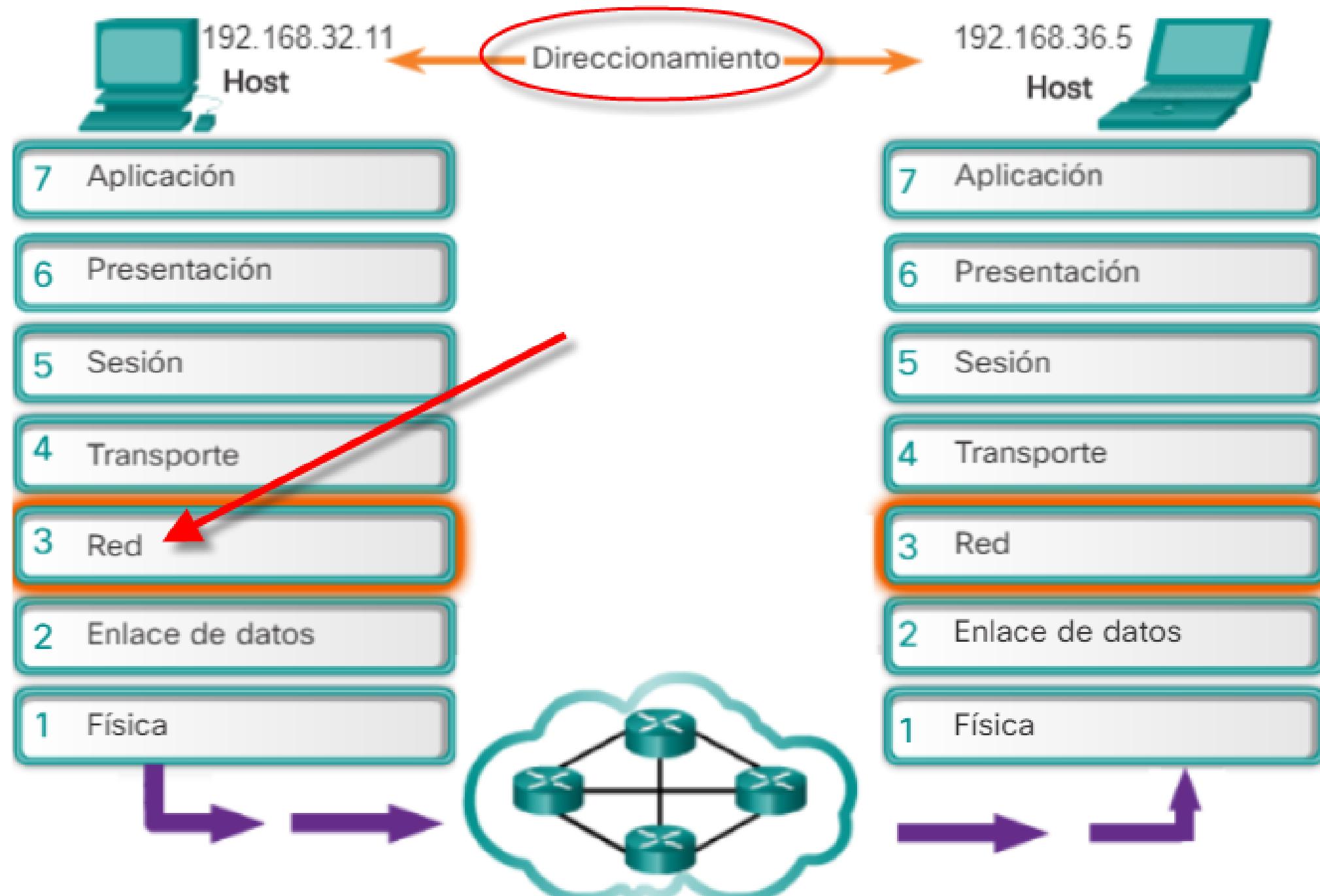
- de **forma independiente**
- pudiendo atravesar **diferentes redes** (redes heterogéneas)
- sin un orden establecido, está es una de las principales **ventajas** de esta arquitectura y por eso es la **base de Internet**.

El **objetivo** principal del nivel de red será **encaminar los paquetes desde el nodo origen hasta el nodo destino**. Cuando los paquetes se tratan de forma independiente, como en **Internet**, **hablamos de una red de commutación de paquetes basada en datagramas, con servicio no orientado a conexión**.

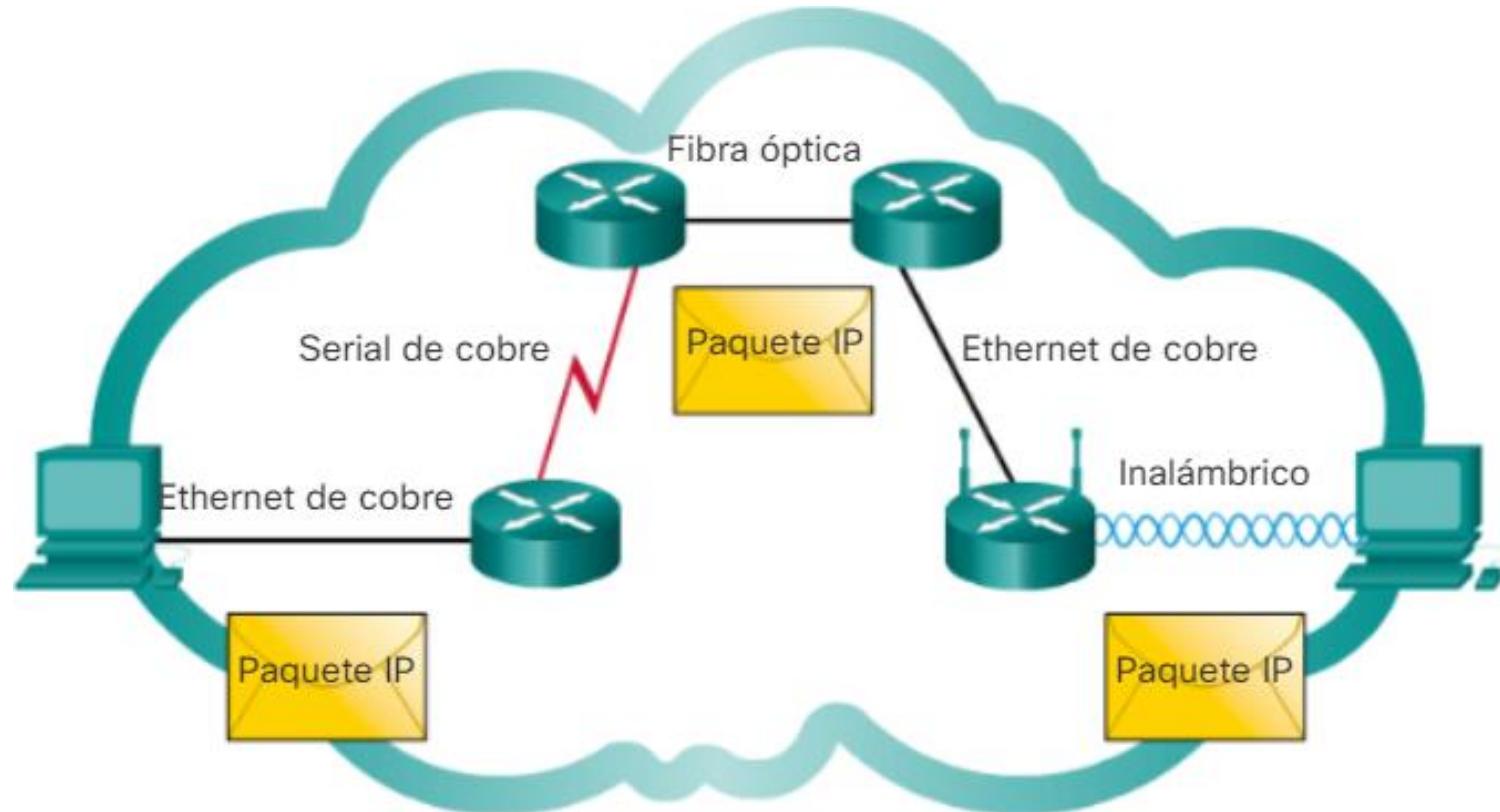
Entre las funciones de la capa de red se encuentra:

- El direccionamiento: permite identificar de forma única cada nodo de la red. Cuando se habla de direccionamiento en este nivel, se está hablando de direcciónamiento lógico, para distinguir del direcciónamiento físico que ya hemos visto anteriormente. Los dispositivos finales deben configurarse con una dirección IP única para su identificación en la red.
- La conectividad: conseguir que los nodos de una red se conecten, independientemente de la red a la que pertenezcan.
- El enrutamiento: También llamado encaminamiento, los protocolos de esta capa deben ser capaces de encontrar el mejor camino entre dos nodos. Un paquete puede **cruzar muchos dispositivos intermediarios** antes de llegar al host de destino. Cada ruta que toma el paquete para llegar al host de destino se denomina “salto”.
- El control de la congestión: Es conveniente realizar un control del tráfico, ya que si un **nodo recibe más información de la que puede procesar, se produce una saturación** y este problema puede extenderse a toda la red.
- **Encapsulación/desencapeculación**: la capa de red recibe una PDU de la capa de transporte.

Agrega la información del encabezado IP, como la dirección IP de los hosts de **origen/destino**. La PDU se denomina “paquete”.



Es responsabilidad de la capa de enlace de datos del modelo OSI tomar un paquete IP y prepararlo para transmitirlo a través del medio de comunicación. Esto significa que el transporte de paquetes IP no está limitado a un medio en particular.



Existe una **característica importante** de los medios que la capa de red tiene en cuenta: el **tamaño máximo de la PDU que cada medio puede transportar**. Esta característica se denomina “unidad máxima de transmisión” (MTU). La **capa de enlace de datos pasa el valor de MTU a la capa de red**. A continuación, la **capa de red determina cuán grandes pueden ser los paquetes**.

El proceso de **encapsulación** de datos capa por capa permite el **desarrollo** y el **escalamiento** de los servicios de las diferentes capas **sin afectar otras capas**. Esto significa que el protocolo IPv4 o IPv6, o cualquier protocolo nuevo que se desarrolle en el futuro, pueden empaquetar fácilmente los segmentos de la capa de transporte.

Encapsulación de la capa de transporte

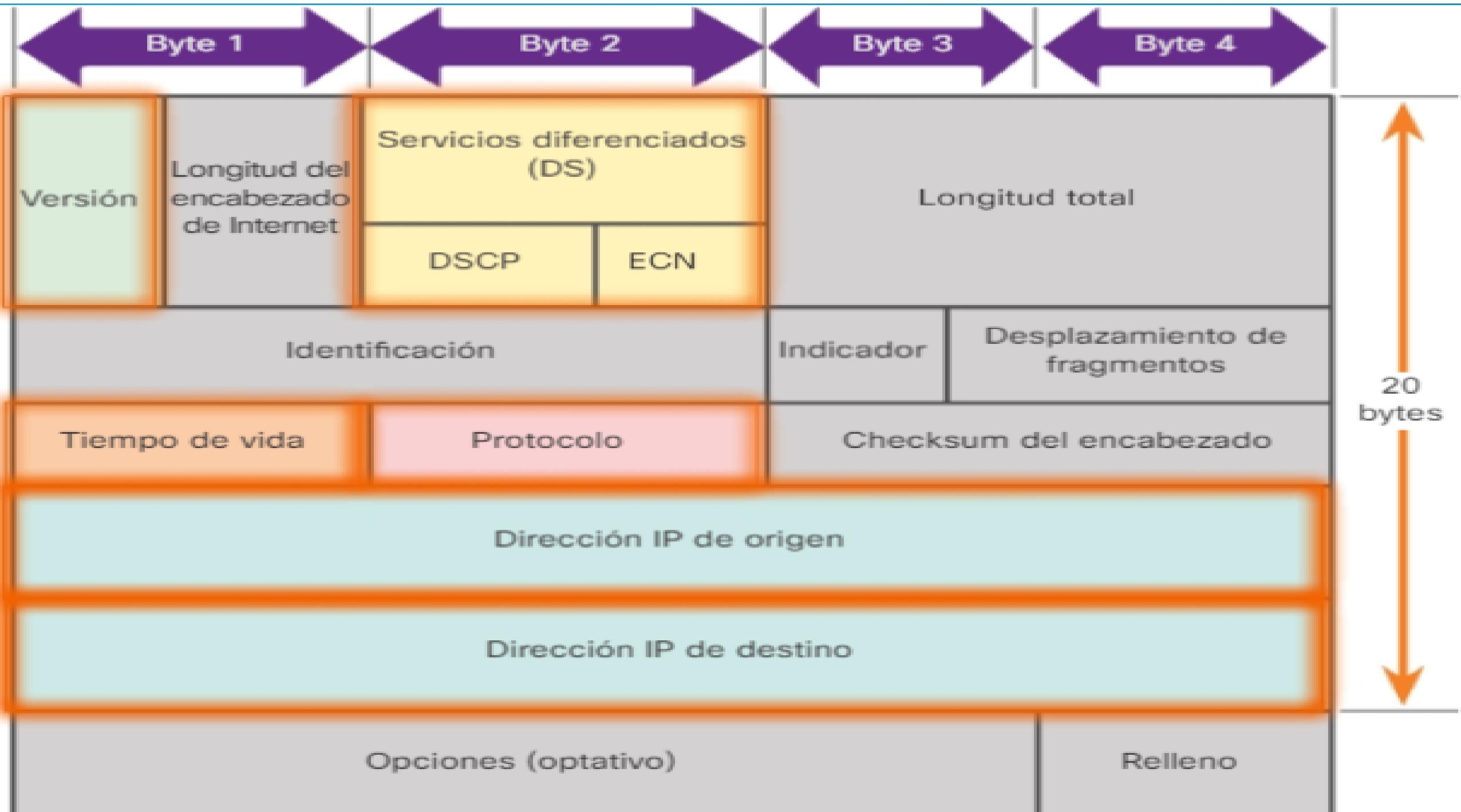


Encapsulación de la capa de red



Los **campos** más importantes del encabezado de IPv4 incluyen los siguientes:

- **Versión:** valor binario de 4 bits que identifica la versión del paquete IP (IPv4).
- **Servicios diferenciados (DS):** campo de 8 bits que se utiliza para **determinar la prioridad** de cada paquete. Utilizado por un mecanismo de calidad de servicio (QoS).
- **Tiempo de vida (TTL):** valor binario de 8 bits que se utiliza para **limitar la vida útil** de un paquete. Se especifica en segundos, comúnmente se denomina “**conteo de saltos**”. El emisor del paquete **establece el valor inicial** de tiempo de vida (TTL), **se disminuye un punto por cada salto**, cada vez que el paquete es procesado por un router. Si el campo TTL disminuye a **cero**, el router **descarta el paquete** y envía un mensaje del protocolo de mensajes de control de Internet (ICMP) de Tiempo superado a la dirección IP de origen.
- **Protocolo:** valor binario de 8 bits indica el **tipo de contenido de datos que transporta** el paquete, lo que permite que la **capa de red pase los datos al protocolo de capa superior correspondiente**, valores comunes incluyen ICMP, TCP y UDP.
- **Dirección IP de origen:** valor binario de 32 bits que representa la dirección IP de origen.
- **Dirección IP de destino:** valor binario de 32 bits que representa la dirección IP de destino.



Para realizar todas estas funciones el nivel de red **utiliza diferentes protocolos**, destacados:

- **IP:** Internet Protocol (Protocolo de Internet) proporciona un **enrutamiento de paquetes no orientado a conexión** a través del **direcccionamiento lógico (direcciones IP)**. Es usado tanto en origen como en destino para comunicación de datos.
- **ICMP:** Protocolo de **mensajes de control en Internet**, suministra capacidades de control y envío de mensajes. Detecta y registra las condiciones de error de la red
- **OSPF:** Protocolo de **enrutamiento que busca el camino más corto entre dos nodos** de la red.
- **EIGRP:** Protocolo de enrutamiento de **vector distancia** avanzado, propiedad de **Cisco Systems**, que ofrece lo mejor de los algoritmos de vector de distancias y del estado de enlace.

Como se puede comprobar este nivel tiene varias funciones, y varios protocolos, pero el más importante de todos, de hecho da nombre a la arquitectura, es el **protocolo IP**.

*Artículos relacionados con el protocolo IP para entender mejor algunos conceptos*

[http://es.wikipedia.org/wiki/Protocolo\\_IP](http://es.wikipedia.org/wiki/Protocolo_IP)

<http://es.wikipedia.org/wiki/IPv4>

<http://es.wikipedia.org/wiki/IPv6>

**Una dirección IP es un número que identifica de manera lógica y jerárquicamente a una interfaz dentro de una red que utilice el protocolo de Internet.**

Existen dos **versiones**:

- **IPv4** (IP versión 4)
- **IPv6** (IP versión 6)

Se diferencian en el número de bits que utilizan, IPv4 utiliza direcciones de 32 bits e IPv6 utiliza direcciones de 128 bits.

**Ejemplo** de direcciones IP son:

- IP versión 4: 192.168.1.11 (valores en **decimal**).
- IP versión 6: 2001:0DB8:0000:0000:0000:1428:57AB (valores en **hexadecimal**) puede **simplificarse** como: 2001:0DB8::1428:57AB)

# El direccionamiento

Es una función **clave** de los protocolos de capa de red que:

- **permite la comunicación de datos entre hosts**
- **proporcionan direcciónamiento jerárquico para los paquetes que transportan datos**

Es independientemente de que:

- los hosts se encuentran en la misma red o en redes diferentes
- **protocolo** de Internet (IPv4 o IPv6)

El diseño, la implementación y la administración de un plan de direcciónamiento IP eficaz asegura que las redes puedan operar de manera eficaz y eficiente.



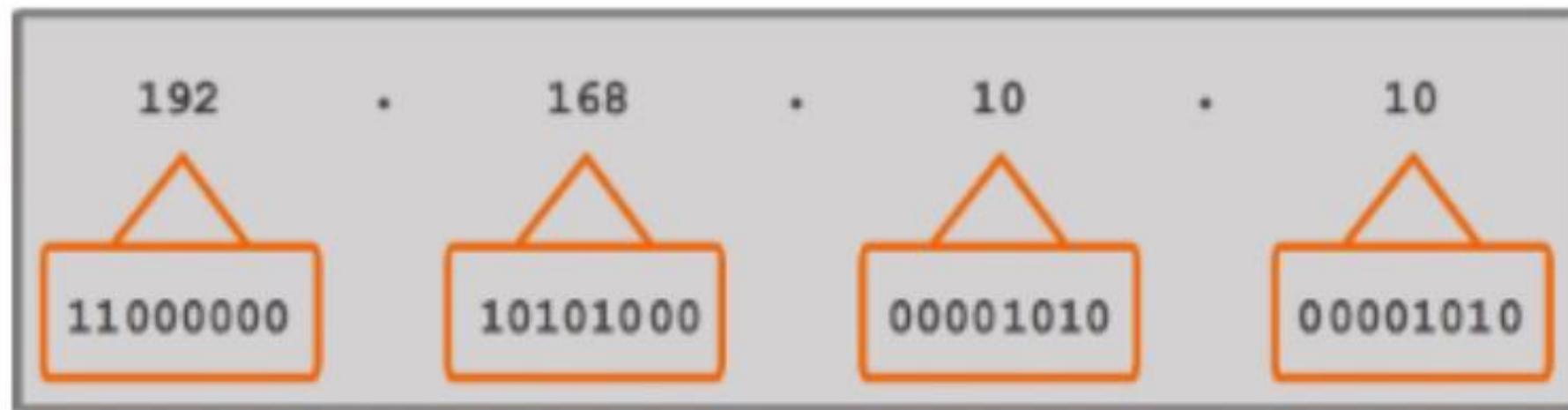
En IPv4, las direcciones son:

- **números binarios de 32 bits.**
- para **facilitar** el uso por parte de las personas, los **patrones binarios** que representan direcciones IPv4 se **expresan en formato decimal punteado**.

Separamos cada byte (8 bits) del patrón binario de 32 bits, llamado “**octeto**”, con un **punto**.

La **dirección binaria**: 11000000 10101000 00001010 00001010

Se expresa como **decimal punteada** de la siguiente manera: 192.168.10.10



Esta dirección está formada por cuatro octetos diferentes.

# Máscara de Subred.

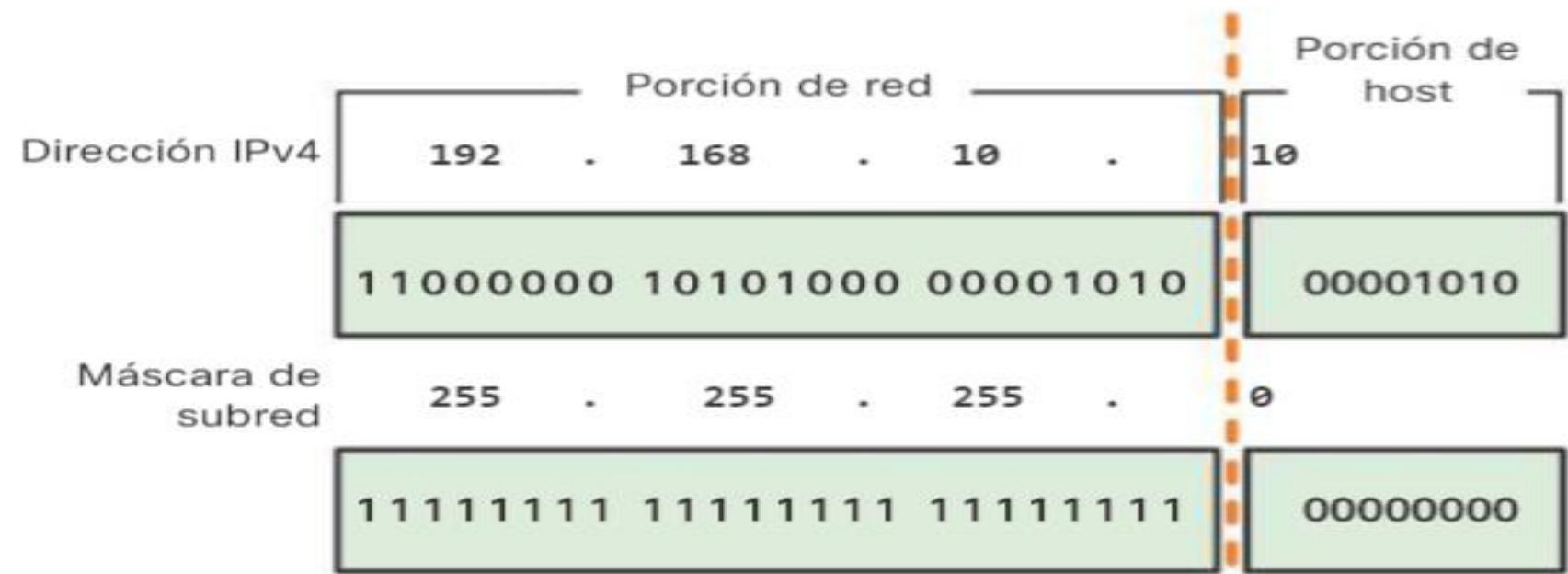
Porción de red y porción de host de una dirección IPv4.

Sirve para **determinar si dos hosts están en la misma red**, para eso es importante entender la notación binaria.

Una dirección IP es una **dirección jerárquica** que consta de dos partes:

- una **porción de red**
- una **porción de host**.

Para determinar la porción de red en comparación con la porción de host, es necesario analizar el conjunto de los 32 bits. Una parte de los bits constituye la **red** y una porción de los bits constituye el **host**.



Los bits dentro de la porción de red de la dirección deben ser idénticos para todos los dispositivos que residen en la misma red.

Los bits dentro de la porción de host de la dirección deben ser únicos para identificar un host específico dentro de una red.

¿Pero cómo saben los hosts qué porción de los 32 bits es red y qué porción es host?  
Esa tarea le corresponde a la máscara de subred.

Cuando se configura un host IP, configuramos:

- una dirección IP
- se asigna una máscara de subred

La máscara de subred tiene una longitud de 32 bits.

Se crea al colocar un 1 binario en cada posición de bit que representa la porción de red y un 0 binario en cada posición de bit que representa la porción de host.

- Los 1 en la máscara de subred representan la porción de red
- Los 0 representan la porción de host.

La máscara de subred no contiene en efecto la porción de red o de host de una dirección IPv4, sino que simplemente le dice al PC dónde buscar estas porciones en una dirección IPv4 dada. Se representa en formato decimal punteado por cuestiones de facilidad de uso. Se configura en un dispositivo host, junto con la dirección IPv4, y es necesaria para que el host pueda determinar a qué red pertenece.

## Prefijos de red

Son otra forma de expresar la máscara de subred.

La **duración de prefijo** es la **cantidad de bits establecidos en 1** en la máscara de subred.

Se escribe en “**notación con barras**”:

- una “/”, establece la **cantidad de bits establecidos en 1**

### Ejemplo

*Si la máscara de subred es 255.255.255.0, hay 24 bits establecidos en 1 en la versión binaria de la máscara de subred:*

*La duración de prefijo es 24 bits o /24.*

El prefijo y la máscara de subred son **diferentes formas de representar lo mismo, la porción de red** de una dirección.

No siempre se asigna un prefijo /24 a las redes. El prefijo asignado puede variar de acuerdo con la cantidad de hosts de la red. Un **número de prefijo diferente cambia el rango de host y la dirección de broadcast para cada red.**

**Hay tres tipos de direcciones dentro del rango de direcciones de cada red IPv4:**

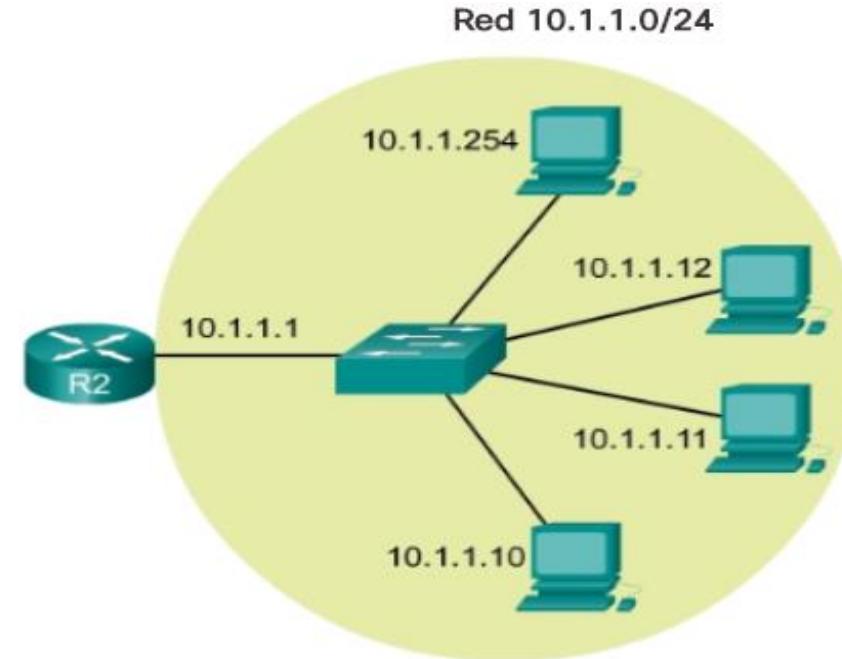
- Dirección de **red**
- Dirección de **host** > primera / última dirección asignables
- Dirección de **broadcast**
- **Dirección de red**

La dirección de red es una **manera estándar de hacer referencia a una red**. Es posible utilizar la **máscara de subred** o la **duración de prefijo**.

$10.1.1.0 // 10.1.1.0$  255.255.255.0 // 10.1.1.0/24

Todos los hosts en la red 10.1.1.0/24 tendrán los mismos bits de porción de red.

Dentro del rango de direcciones IPv4 de una red, la **primera dirección se reserva para la dirección de red**. Esta dirección tiene un **0** para cada bit de host en la **porción de host** de la dirección. Todos los hosts dentro de la red **comparten la misma dirección de red**.



- Dirección de host

Cada dispositivo final requiere una dirección única para comunicarse en la red.

Esta dirección tiene **cualquier combinación de bits 0 y bits 1 en la porción de host de la dirección, pero no puede contener todos bits 0 o todos bits 1.**



- Dirección de broadcast

Es una **dirección especial** para cada red que permite la **comunicación a todos los host en esa red**. Un host puede enviar un único paquete dirigido a la dirección de broadcast de la red, y cada host en la red que recibe este paquete procesa su contenido.

Utiliza la **dirección más alta en el rango de la red**, los **bits de la porción de host son todos 1**.

Todos 1 en un octeto en forma binaria es igual al número 255 en forma decimal.

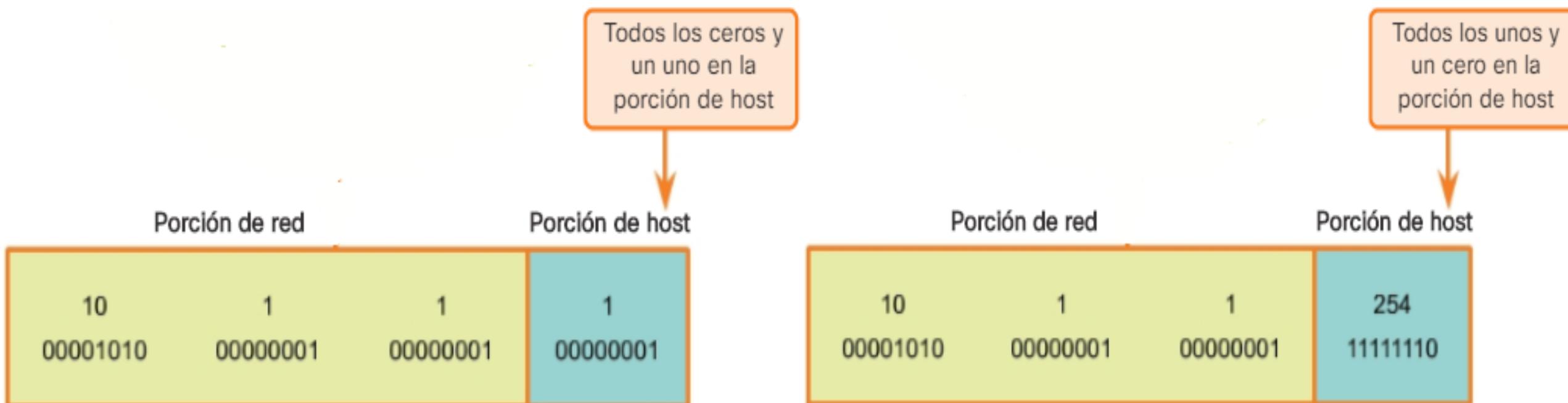


- **Primera dirección de host**

La porción de host de la **primera dirección de host** contiene **todos bits 0 con un bit 1 que representa el bit de orden más bajo** o el bit que está más a la derecha. En muchos esquemas de direccionamiento, es común utilizar la primera dirección de host del router o la dirección de gateway predeterminado.

- **Última dirección de host**

La porción de host de la **última dirección de host** contiene **todos bits 1, con un bit 0 que representa el bit de orden más bajo** o el bit que está más a la derecha.



Observar distintos prefijos que se utilizan sobre la misma dirección 10.1.1.0.

Observar que la **dirección de red** puede permanecer igual, pero el **rango de host y la dirección de broadcast** son diferentes para las **diferentes duraciones de prefijos**.

Dirección de Red: 10.1.1.0/24

Dirección de red	10.1.1.0/24	10.1.1.00000000
Primera dirección de host	10.1.1.1	10.1.1.00000001
Última dirección de host	10.1.1.254	10.1.1.11111110
Dirección de broadcast	10.1.1.255	10.1.1.11111111
Cantidad de hosts: $2^8 - 2 = 254$ hosts		

Dirección de red	<b>10.1.1.0/25</b>	<b>10.1.1.00000000</b>
Primera dirección de host	<b>10.1.1.1</b>	<b>10.1.1.00000001</b>
Última dirección de host	<b>10.1.1.126</b>	<b>10.1.1.01111110</b>
Dirección de broadcast	<b>10.1.1.127</b>	<b>10.1.1.01111111</b>
Cantidad de hosts: $2^7 - 2 = 126$ hosts		

Dirección de red	<b>10.1.1.0/26</b>	<b>10.1.1.00000000</b>
Primera dirección de host	<b>10.1.1.1</b>	<b>10.1.1.00000001</b>
Última dirección de host	<b>10.1.1.62</b>	<b>10.1.1.00111110</b>
Dirección de broadcast	<b>10.1.1.63</b>	<b>10.1.1.00111111</b>
Cantidad de hosts: $2^6 - 2 = 62$ hosts		

Dirección de red	<b>10.1.1.0/27</b>	<b>10.1.1.00000000</b>
Primera dirección de host	<b>10.1.1.1</b>	<b>10.1.1.00000001</b>
Última dirección de host	<b>10.1.1.30</b>	<b>10.1.1.00011110</b>
Dirección de broadcast	<b>10.1.1.31</b>	<b>10.1.1.00011111</b>
Cantidad de hosts: $2^5 - 2 = 30$ hosts		

Dirección de red	<b>10.1.1.0/28</b>	<b>10.1.1.00000000</b>
Primera dirección de host	<b>10.1.1.1</b>	<b>10.1.1.00000001</b>
Última dirección de host	<b>10.1.1.14</b>	<b>10.1.1.00001110</b>
Dirección de broadcast	<b>10.1.1.15</b>	<b>10.1.1.00001111</b>
Cantidad de hosts: $2^4 - 2 = 14$ hosts		

Cuando se asigna una dirección IPv4 a un dispositivo, ese dispositivo utiliza la **máscara de subred** para determinar a qué dirección de red pertenece.

Al enviar datos de red, el dispositivo **utiliza esta información para determinar si puede enviar paquetes localmente o si debe enviarlos a un gateway predeterminado para la entrega remota**.

Cuando un **host envía un paquete**, compara la porción de red de su propia dirección IP con la porción de red de la dirección IP de destino.

- Si los bits de la red coinciden, están en la misma red, y el paquete puede ser enviado **localmente**.
- Si no coinciden, el host emisor **reenvía el paquete al gateway** predeterminado para que se envíe a otra red. Deben tener un dispositivo de capa3 (un router) entre ellas para comunicarse.

La **operación AND** se usa para determinar la dirección de red. La lógica AND es la comparación de dos bits que produce los siguientes resultados:

- $1 \text{ AND } 1 = 1$  (*figura 1*)
- $0 \text{ AND } 1 = 0$  (*figura 2*)
- $0 \text{ AND } 0 = 0$  (*figura 3*)
- $1 \text{ AND } 0 = 0$  (*figura 4*)

## En una red IPv4, los hosts pueden comunicarse de una de tres maneras:

- **Unicast**: proceso por el cual se envía un paquete de un host a un host individual.
- **Broadcast**: proceso por el cual se envía un paquete de un host a todos los hosts en la red.  
Dirección: 255.255.255.255, los routers separan dominios de broadcast para mejorar el rendimiento de la red
- **Multicast**: proceso por el cual se envía un paquete de un host a un grupo seleccionado de hosts, posiblemente en redes distintas.

Direcciones IPv4 multicast son 224.0.0.0 a 224.0.0.255. Los hosts que reciben **datos multicast específicos** se denominan “clientes multicast”. Los clientes multicast utilizan servicios solicitados por un programa cliente para **subscribirse** al grupo multicast.

*Ejemplo*: se reservó 224.0.1.1 para que el protocolo de hora de red (NTP) sincronice los relojes con la hora del día de los dispositivos de red.

[Mostrar Recurso 8.1.3.3 – 8.1.3.5](#)

[Actividad 8.1.3.7 Cálculo dirección de red, broadcast, host](#)

Dirección suministrada/prefijo **147.88.61.36/21**

Tipo de dirección	Introduzca el último octeto del prefijo de red en valores binarios	Introduzca el ÚLTIMO octeto en valores decimales	Introduzca la dirección completa en valores decimales
Red	<input type="text"/>	<input type="text"/>	<input type="text"/>
Broadcast	<input type="text"/>	<input type="text"/>	<input type="text"/>
Primera dirección de host utilizable	<input type="text"/>	<input type="text"/>	<input type="text"/>
Última dirección de host utilizable	<input type="text"/>	<input type="text"/>	<input type="text"/>

# Dirección suministrada/prefijo 147.88.61.36/21

Tipo de dirección	Introduzca el último octeto del prefijo de red en valores binarios	Introduzca el ÚLTIMO octeto en valores decimales	Introduzca la dirección completa en valores decimales
Red	00000000	0	147.88.56.0
Broadcast	11111111	255	147.88.63.255
Primera dirección de host utilizable	00000001	1	147.88.56.1
Última dirección de host utilizable	11111110	254	147.88.63.254

11111111 11111111 11111000 00000000 /21 máscara de subred 255.255.248.0

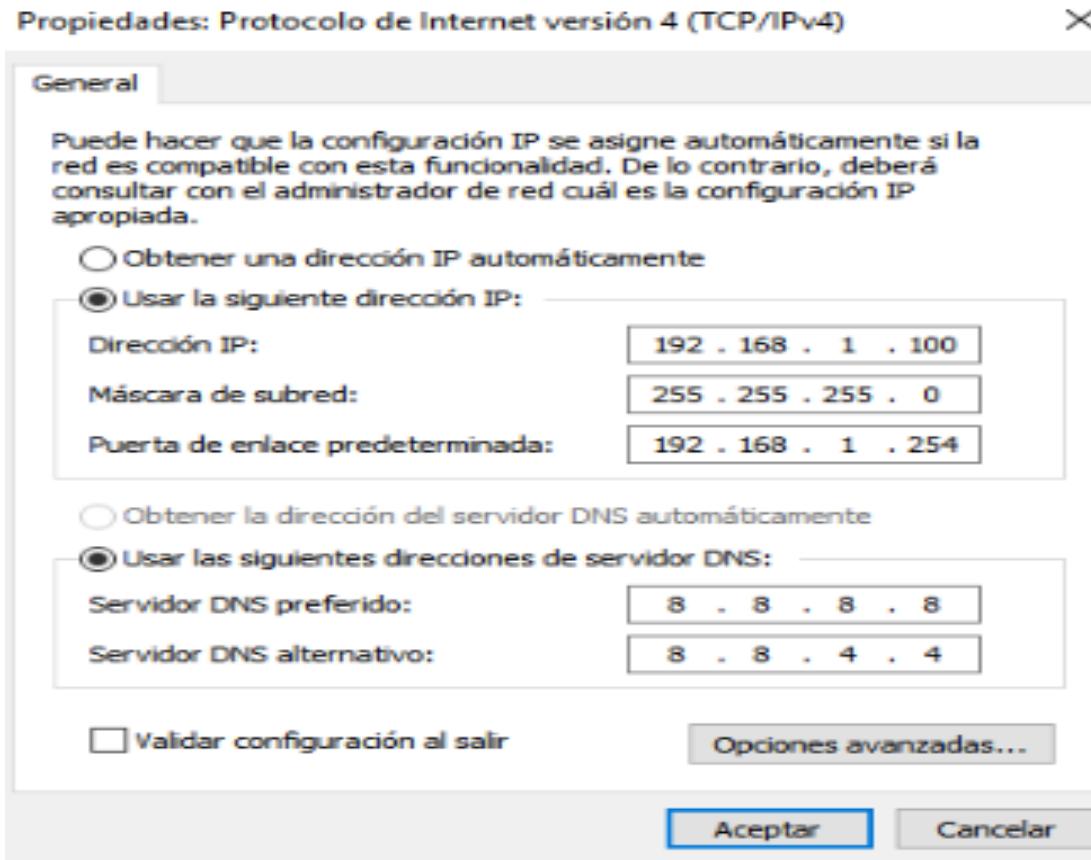
10010011 01011000 00111/101 00100100 dirección suministrada: **147.88.61.36**

10010011 01011000 00111000 00000000 dirección de red: **147.88.56.0**

En la mayoría de las redes de datos, **la mayor población de hosts incluye dispositivos finales**, como PC, tablet PC, smartphones, impresoras y teléfonos IP. Debe **asignarse la mayor cantidad de direcciones a estos hosts** >>> direcciones IP del rango de direcciones disponibles en la red.

Pueden asignarse de manera **estática o dinámica**.

- **Asignación estática:** El administrador de red debe **configurar manualmente la información de red para un host**.



#### Ventajas:

- Para impresoras, servidores y otros **dispositivos de red que no suelen cambiar la ubicación** y que deben ser accesibles para los clientes en la red sobre la base de una dirección IP fija.
- Puede proporcionar un **mayor control** de los recursos de red. Por ejemplo, es posible crear filtros de acceso sobre la base del tráfico desde y hacia una dirección IP específica.

#### Desventajas:

- Introducir el direccionamiento estático en cada host **puede llevar mucho tiempo**.
- Es necesario mantener una **lista precisa de las direcciones IP asignadas** a cada dispositivo.

- Asignación dinámica:

Es habitual que la **población de usuarios cambie frecuentemente**. Se agregan nuevos usuarios con computadoras **portátiles**, y esos usuarios requieren una conexión.

Otros tienen estaciones de trabajo nuevas u otros dispositivos de red, como **smartphones**, que deben conectarse.

En lugar de que el administrador de red asigne direcciones IP para cada estación de trabajo, es más simple que las **direcciones IP se asignen automáticamente**. Esto se realiza mediante un **protocolo conocido como Protocolo de configuración dinámica de host (DHCP)**.

**El DHCP permite la asignación automática de información de direccionamiento**

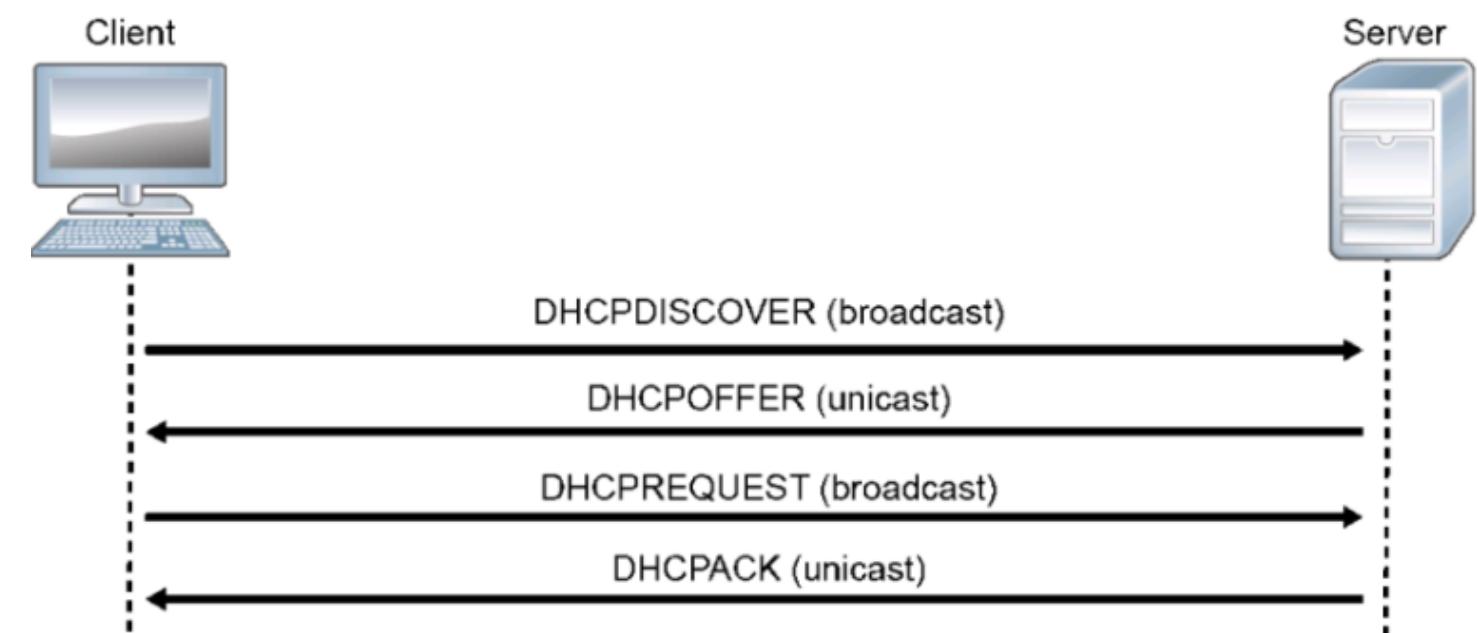
- dirección IP
- máscara de subred
- gateway predeterminado
- otra información de configuración

La **configuración** del servidor de DHCP requiere que se utilice un bloque de direcciones, denominado “**conjunto de direcciones**”, para la asignación a los clientes DHCP en una red.

Deben planificarse de modo que excluyan cualquier dirección estática que utilicen otros dispositivos.

## Ventajas:

- reduce la **carga** para al personal de soporte de la red
- elimina los **errores** de entrada
- 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** >>> útil para los usuarios móviles que entran y salen de la red



## Direcciones IPv4 públicas y privadas

- **Direcciones privadas:** los bloques de direcciones de **espacio privado** se utilizan en redes privadas. Los hosts que **no requieren acceso a Internet** pueden utilizar direcciones privadas. Sin embargo, **dentro de la red privada, los hosts aún requieren direcciones IP únicas dentro del espacio privado.**

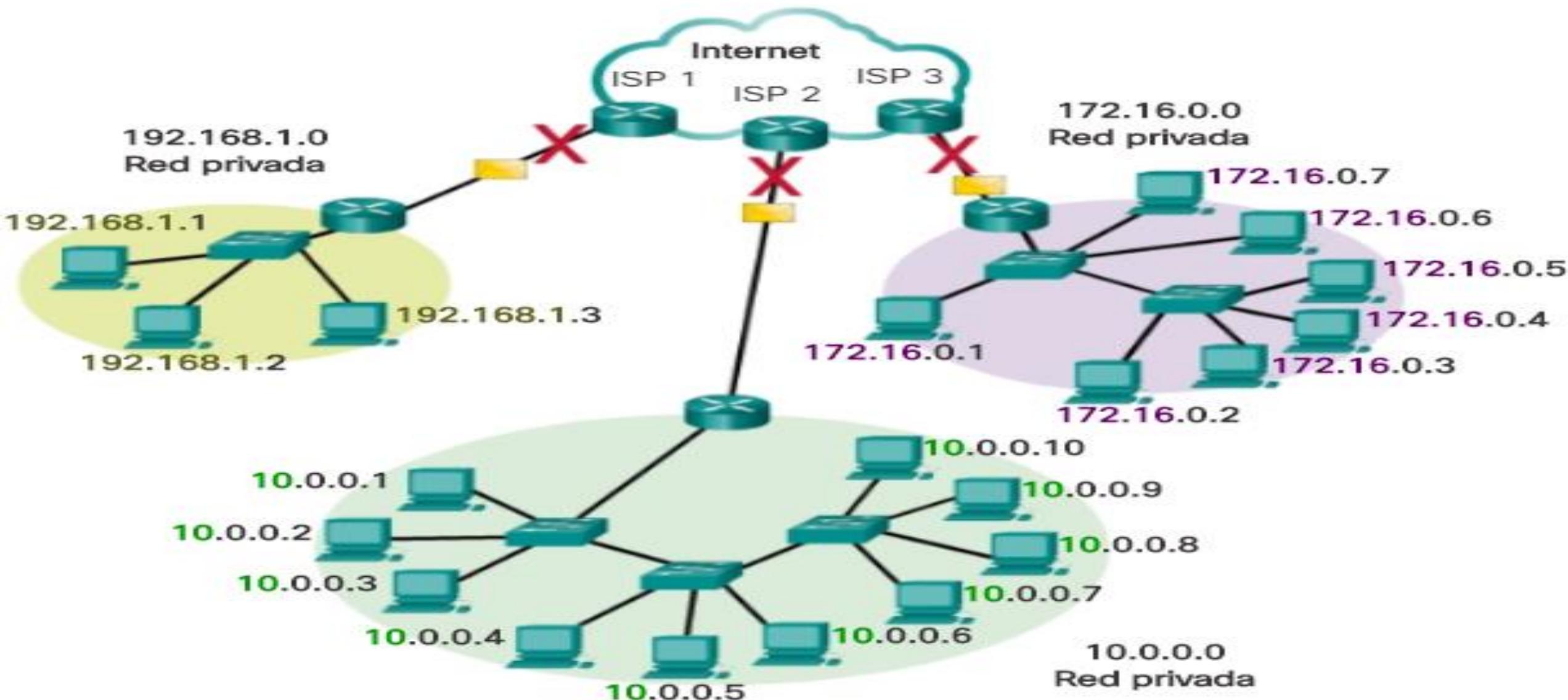
Los **bloques** de direcciones privadas son:

- **10.0.0.0 a 10.255.255.255 (10.0.0.0/8)**
- **172.16.0.0 a 172.31.255.255 (172.16.0.0/12)**
- **192.168.0.0 a 192.168.255.255 (192.168.0.0/16)**

**Hosts en distintas redes pueden utilizar las mismas direcciones de espacio privado.** Los paquetes que utilizan estas direcciones como la dirección de origen o de destino **no deberían aparecer en la Internet pública.** El router del perímetro de estas redes privadas deben **bloquear o convertir** estas direcciones.

- **Direcciones públicas:** diseñadas para ser utilizadas en los hosts de acceso público desde Internet.

Las direcciones privadas no se pueden enrutar a través de Internet.



## Direcciones Especiales:

- **Loopback**: 127.0.0.1. , es una dirección que los hosts utilizan para **dirigir el tráfico hacia ellos mismos**. Crea un método de acceso directo para las **aplicaciones y servicios TCP/IP que se ejecutan en el mismo dispositivo para comunicarse entre sí**.
  - Al utilizar la dirección de loopback en lugar de la dirección host IPv4 asignada, dos servicios en el mismo host pueden **desviar las capas inferiores del stack de TCP/IP**.
  - También es posible hacer ping a la dirección de loopback para **probar la configuración de TCP/IP** en el host local.

Se reservan las **direcciones 127.0.0.0 a 127.255.255.255**. Cualquier dirección dentro de este bloque producirá un loopback al host local. Las direcciones dentro de este bloque **no deben figurar en ninguna red**.

- **Direcciones link-local**: va de 169.254.0.0 a 169.254.255.255 (169.254.0.0/16). El sistema operativo puede asignar automáticamente estas direcciones al host local en entornos donde no se dispone de una configuración IP. Se pueden utilizar en una red punto a punto pequeña o para un host que no pudo obtener una dirección de un servidor de DHCP automáticamente. (protocolo **APIPA**)
- **Direcciones experimentales**: va de 240.0.0.0 a 255.255.255.254 reservadas para **uso futuro**, para fines de **investigación o experimentación**, y **no se pueden utilizar** en una red IPv4.

## Servicios del ISP

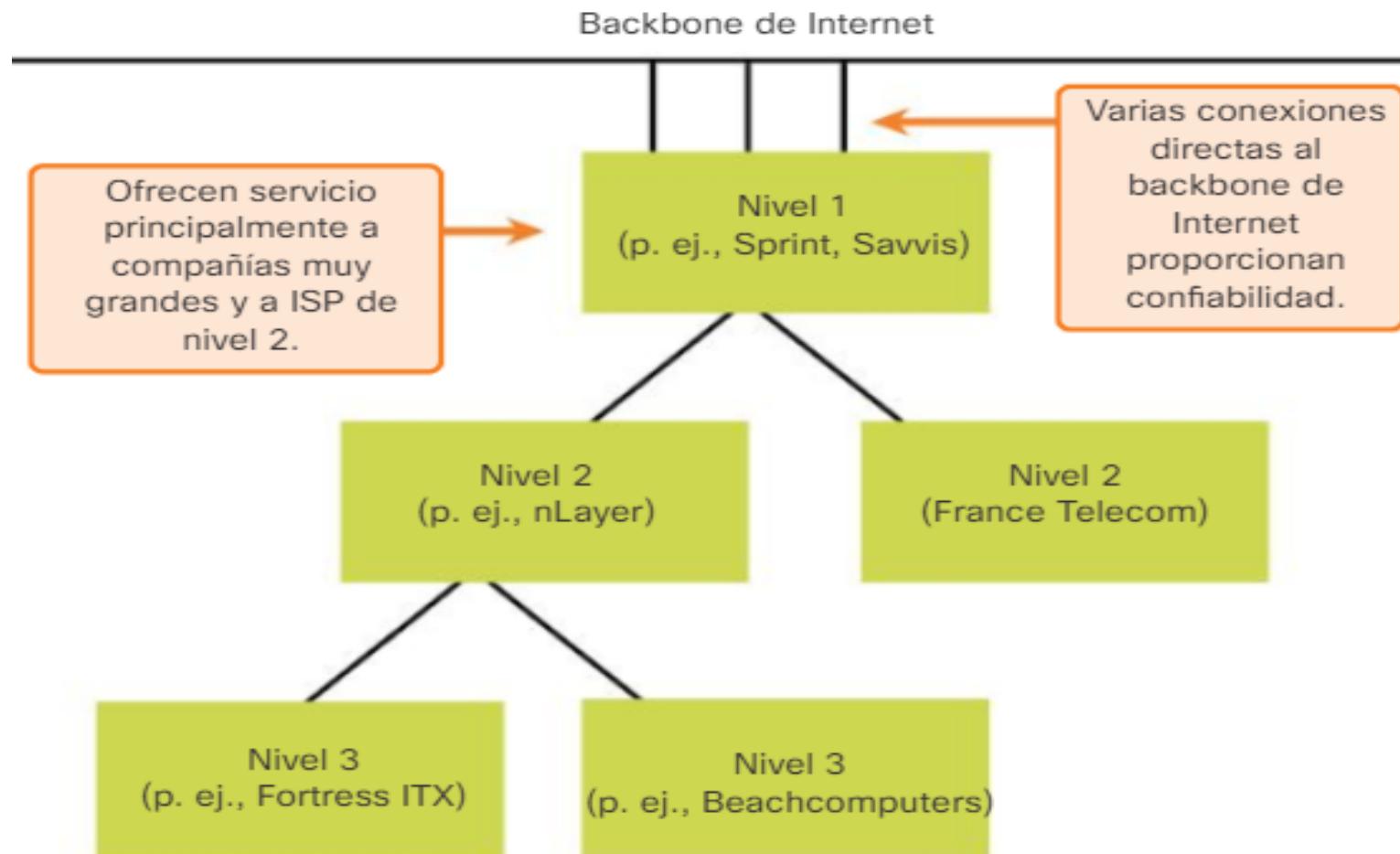
Para tener acceso a los **servicios de Internet**, tenemos que conectar nuestra red de datos a **Internet usando un proveedor de servicios de Internet (ISP)**. Poseen sus propios conjuntos de redes internas de datos para administrar conectividad a Internet y ofrecer servicios relacionados.

### Niveles del ISP

Se designan mediante una **jerarquía basada en su nivel** de conectividad al **backbone** de Internet. Cada **nivel inferior obtiene conectividad al backbone por medio de la conexión a un ISP de nivel superior**.

- **Nivel 1:** cima de la jerarquía de ISP.
  - Grandes ISP a nivel nacional/internacional se conectan directo al backbone de Internet.
  - **Clientes** de ISP de nivel 1 son **ISP de menor nivel o grandes compañías**
  - Conexiones y servicios altamente **confiables**.
  - Alta **velocidad**.
- **Nivel 2:** adquieren su servicio de Internet de los ISP de nivel 1.
  - Se centran en los clientes empresa.
  - Ofrecen **más servicios** que los ISP de los otros dos niveles.
  - Acceso **más lento** a Internet
  - **Menor confiabilidad** que los IPS de Nivel 1.

- **Nivel 3:** adquieren su servicio de Internet de los ISP de nivel 2.
  - El objetivo de estos ISP son los **mercados minoristas** y del **hogar** en una ubicación específica
  - Su necesidad principal es **conectividad y soporte**
  - Tienen un **menor ancho de banda y menos confiabilidad** que los proveedores de nivel 1 y 2, pero suelen ser buenas opciones para pequeñas y medianas empresas.



# CLASES DE DIRECCIONES

CLASE	DIRECCIONES DISPONIBLES		CANTIDAD DE REDES	CANTIDAD DE HOSTS
	DESDE	HASTA		
A	0.0.0.0	127.255.255.255	128*	16.777.214
B	128.0.0.0	191.255.255.255	16.384	65.534
C	192.0.0.0	223.255.255.255	2.097.152	254
D	224.0.0.0	239.255.255.255	no aplica	no aplica
E	240.0.0.0	255.255.255.255	no aplica	no aplica

0 - 127      **01001011** . **00111101** . **10101001** . **01000100**      Clase A  
 128 - 191     **10011011** . **00111101** . **10101001** . **01000100**      Clase B  
 192 - 223     **11011011** . **10001111** . **10101001** . **01000100**      Clase C

Primer octeto		Direcciones IP				
Primeros bits	Rango de valores	CLASE	Máscara de red	Red y máquina	Número de Redes	Número de máquinas ó hosts
0	0-127	A	255.0.0.0	N.h.h.h	$2^7=128$	16.777.214
10	128-191	B	255.255.0.0	N.N.h.h	$2^{14}=16.384$	65.534
110	192-223	C	255.255.255.0	N.N.N.h	$2^{21}=2.097.152$	254
1110	224-239	D	No aplicable	Reservado	No aplicable	No aplicable
1111	240-255	E	No aplicable	Reservado	No aplicable	No aplicable

- **Clase A**: clase es para las **redes muy grandes**, tales como las de una gran compañía internacional. Las direcciones del IP con un **primer octeto** del 0 al 127 son parte de esta clase. **Los otros tres octetos son usados para identificar cada anfitrión**. Esto significa que hay **126** (quitando la **0.0.0.0** y la **127.0.0.0**) **redes de la clase A con  $16.777.214 (2^{24} - 2)$  posibles anfitriones** para un total de **2.147.483.648 ( $2^{31}$ )** direcciones únicas IP. En redes de la clase A, el primer número binario en el primer octeto es **siempre 0**.
- **Clase B**: clase B se utiliza para las **redes de tamaño mediano** (**campus grande de la universidad**). Las direcciones IP con un primer octeto a partir del 128 a 191 son parte de esta clase. También incluyen el segundo octeto como parte del identificador neto. Utilizan los otros **dos octetos para identificar cada anfitrión (host)**. Esto significa que hay **16.384 ( $2^{14}$  dos bits para identificar clase B -<sub>10</sub>- )** **redes de la clase B con  $65.534 (2^{16} - 2)$  anfitriones posibles** cada uno para un total de **1.073.741.824 ( $2^{30}$ )** direcciones únicas IP.

- **Clase C:** se utilizan para **negocios pequeños/mediano** tamaño. Las direcciones IP con un primer octeto del 192 al 223 son parte de esta clase. Incluyen a segundos y terceros octetos como parte del identificador neto. Utilizan al **último octeto para identificar cada anfitrión**. Esto significa que hay  $2.097.152 (2^{21})$  redes de la clase C con  $254 (2^8 - 2)$  anfitriones posibles cada uno para un total de  $536.870.912 (2^{29})$  direcciones. Tienen un primer bit **valor de 1, segundo bit 1 y de un tercer bit 0 en el primer octeto.**
- **Clase D:** utilizado para los **multicast**, la clase D es levemente diferente de las primeras tres clases. Tiene un primer bit con valor de 1, segundo bit 1, tercer bit 1 y cuarto bit 0. Los otros 28 bits se utilizan para identificar el grupo de computadoras al que el mensaje del multicast esta dirigido.
- **Clase E:** se utiliza para propósitos **experimentales** solamente. Tiene un primer bit valor de 1, segundo bit 1, tercer bit 1 y cuarto bit 1. Los otros 28 bits se utilizan para identificar el grupo de computadoras que el mensaje del multicast esta dirigido.

# Limitaciones de IPv4

A través de los años, IPv4 se actualizó para enfrentar nuevos desafíos, pero continúa teniendo **tres problemas importantes:**

- **Agotamiento de direcciones IP:** IPv4 dispone de una cantidad limitada de direcciones IP públicas exclusivas.
- **Expansión de la tabla de enrutamiento de Internet:** los **routers utilizan tablas de enrutamiento** para determinar cuál es el mejor camino. Las rutas IPv4 consumen muchos recursos de memoria y de procesador en los routers de Internet.
- **Falta de conectividad de extremo a extremo:** la **traducción de direcciones de red (NAT)** proporciona una forma de que varios dispositivos comparten una misma dirección IP pública. Sin embargo, dado que comparten la dirección IP pública, la dirección IP de un host de red interno se oculta. Esto puede resultar **problemático para las tecnologías que requieren conectividad de extremo a extremo.**



## RFC (Request For Comments) o solicitud de comentarios:

- documento que puede ser **escrito por cualquier persona**.
- contiene una **propuesta** para una nueva **tecnología**, información acerca del uso de tecnologías y/o recursos existentes, propuestas para mejoras de tecnologías, proyectos experimentales y demás.
- conforman básicamente la documentación de **protocolos y tecnologías de Internet**, siendo incluso muchas de ellas estándares.
- mantenidas por el **IETF** (Internet Engineering Task Force)
- **accesibles** por cualquier persona >>> son publicadas online y sin restricciones.
- asignan a cada una un **número único** que la identifique y que es el **consecutivo** de la última RFC publicada. Una RFC ya publicada **jamás puede modificarse**, no existen varias versiones de una RFC. Lo que se hace es escribir una nueva RFC que **deje obsoleta o complemente** una RFC anterior.

Para **crear** una nueva RFC puede utilizarse el **sitio RFC Editor**, donde se envían las nuevas propuestas que eventualmente podrán ser adoptadas como RFC y, si son de gran interés, convertirse en estándares <https://www.rfc-editor.org/>

Especificación	RFC
Protocolo IP	<a href="#">RFC791</a>
Protocolo ICMP (Protocolo de mensajes de control de Internet)	<a href="#">RFC792</a>
Protocolo TCP (Protocolo de control de transmisión)	<a href="#">RFC793</a>
Protocolo FTP (Protocolo de transferencia de archivos)	<a href="#">RFC959</a>
Correo electrónico	<a href="#">RFC822</a>
Protocolo Telnet	<a href="#">RFC854</a>
Protocolo NNTP (transferencia de noticias a través de la red)	<a href="#">RFC977</a>
TCP/IP	<a href="#">RFC1180</a>
Preguntas frecuentes para principiantes	<a href="#">RFC1206</a>
Glosario de la red	<a href="#">RFC1208</a>
Asignación de direcciones IP para Intranet	<a href="#">RFC1597</a>
Protocolo PPP (Protocolo punto a punto)	<a href="#">RFC1661</a>
Números de puerto	<a href="#">RFC3232</a>
Protocolo HTTP	<a href="#">RFC2068</a>
Protocolo SMTP (Protocolo simple de transferencia de correo)	<a href="#">RFC2821</a>

### The RFC series

contains technical and organizational documents about the Internet, including the specifications and policy documents produced by four streams: the Internet Engineering Task Force ([IETF](#)), the Internet Research Task Force ([IRTF](#)), the Internet Architecture Board ([IAB](#)), and Independent Submissions.

[Browse the RFC Index](#)

[HTML \(ascending\)](#) • [HTML \(descending\)](#) • [TXT](#) • [XML](#)

Note: These files are large.

[Browse RFCs by Status](#)

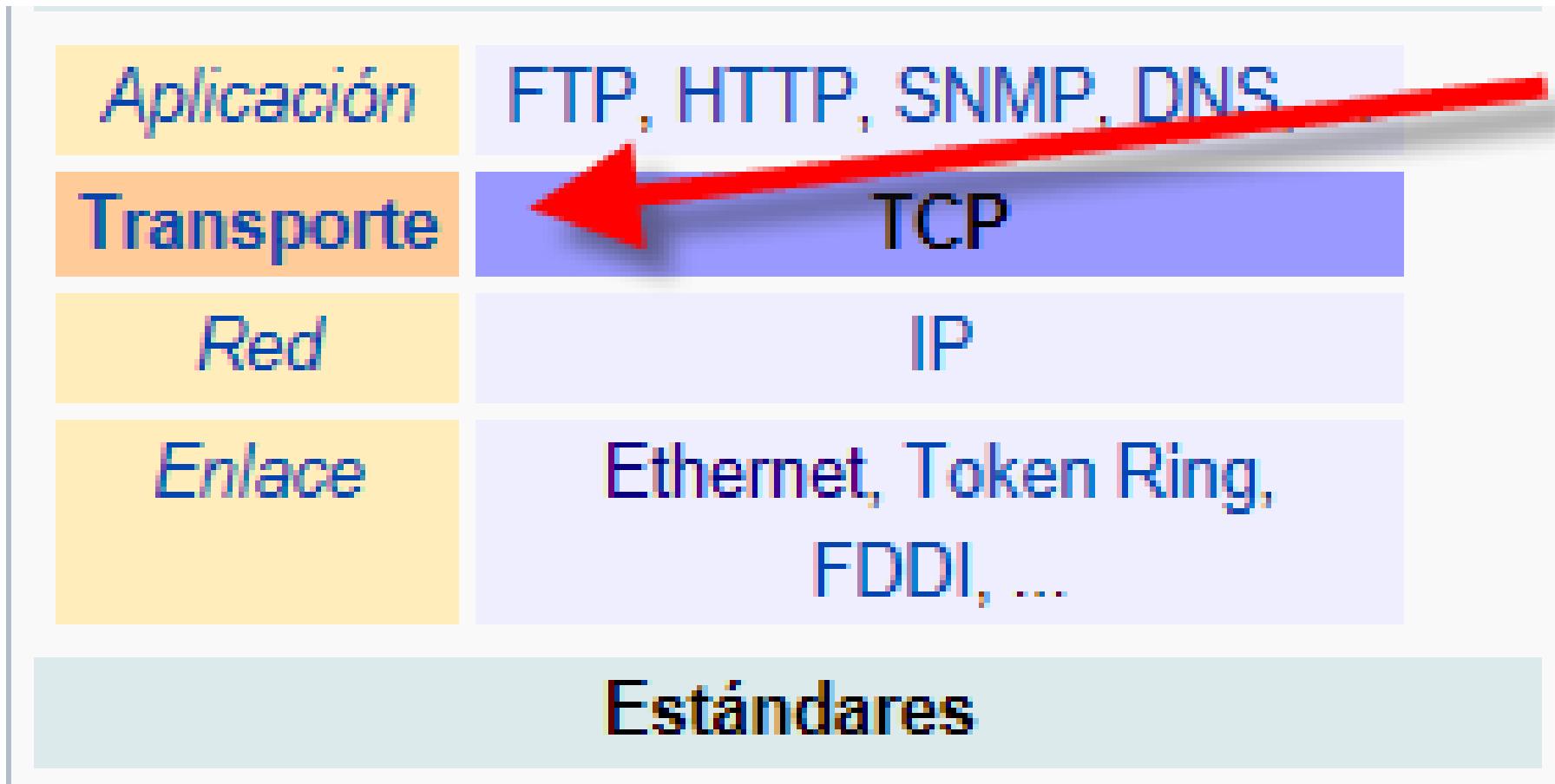
Internet Standard

Actividad. Introduce en el Explorador Internet Protocol.

# Capa3 o Capa de Transporte.

Cumple la función de:

- establecer las reglas necesaria para establecer una conexión entre dos dispositivos remotos
- unir múltiples segmentos del mismo flujo de datos



Las **aplicaciones** como: clientes de correo electrónico, exploradores Web y clientes de mensajería instantánea, permiten que las **personas usen dispositivos y redes para enviar mensajes y encontrar información.**

Los **datos** de cada una de estas aplicaciones se **empaquetan**, se **transportan** y se **entregan** a la aplicación correspondiente en el **dispositivo de destino**.

Como en capas anteriores, la **información (PDU)** que maneja esta capa tiene su nombre:

## **Segmento**

En esta capa es donde se deben cuidar **detalles como el orden de los paquetes y control de errores.**

Los **procesos** que se describen en la capa de transporte del modelo OSI:

- **aceptan los datos de la capa de aplicación >>> capa superior**
- **los preparan para el direccionamiento en la capa de red >>> capa inferior**

Un PC de origen se comunica con PC receptor para establecer el conjunto de reglas, funciones:

- cómo **dividir** los datos en segmentos
- **mantener el flujo** de la red
- transporte **independientemente** de las redes físicas
- permite que varias aplicaciones se puedan comunicar a través la red al **mismo tiempo** en un **único dispositivo**, se realiza un rastreo de comunicación individual entre aplicaciones en los hosts de origen y destino
- identificación de la aplicación correspondiente para cada stream de comunicación



La capa de transporte garantiza que aunque sean varias las aplicaciones se ejecutan en un dispositivo, todas reciban los datos correctos.

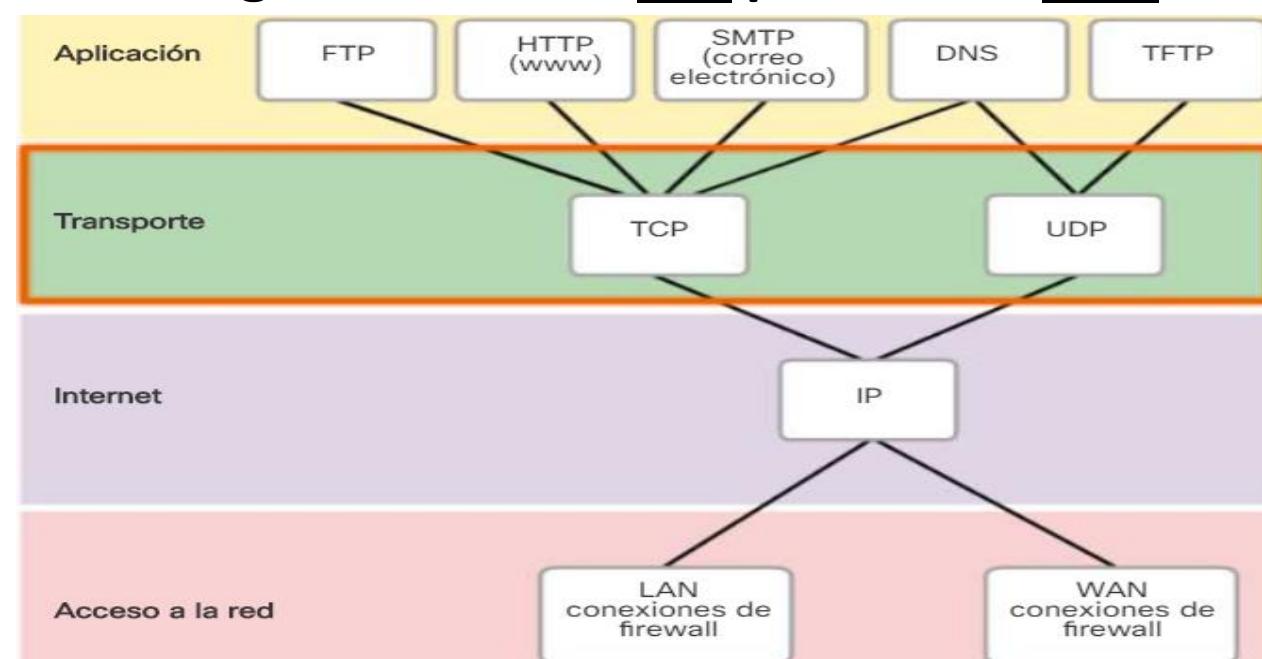
**Ejemplo:** Al considerar la capa de transporte, imagíñese un departamento de envíos que prepara un único pedido de varios paquetes para entregar.

La capa de transporte **proporciona**:

- un **método** para entregar datos a través de la red de manera que **garantiza que estos se puedan volver a unir** correctamente en el extremo **receptor** >>> **orden** de los segmentos
- el control necesario para **rearmar estos segmentos en los distintos streams de comunicación**
- método para verificar si los datos llegan correctos >>> **control de errores**

Estos procesos de segmentación y rearmado se pueden lograr utilizando **dos protocolos muy diferentes de la capa de transporte**:

- el protocolo de control de transmisión (TCP)
- el protocolo de datagramas de usuario (UDP)



## TCP

- Protocolo de transporte **confiable**: incluye **procesos que garantizan la entrega confiable** entre aplicaciones, mediante el uso de **tres operaciones básicas** de confiabilidad:
  - **Seguimiento** de segmentos de datos transmitidos
  - **Acuse** de recibo de datos
  - **Retransmisión** de cualquier dato sin acuse de recibo, caso de error

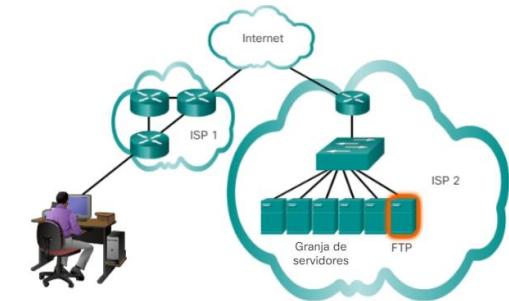
*Ejemplo: Similar al envío de paquetes de los que se hace un seguimiento de origen a destino.*

Forma de proceder, **funcionamiento**:

- TCP **divide el mensaje en partes pequeñas**, conocidas como **segmentos**.
- Los segmentos se **numeran en secuencia y se pasan al proceso IP para armarse en paquetes**.
- TCP **realiza un seguimiento** del número de segmentos que se enviaron a un host específico desde una aplicación específica. Si el **emisor no recibe un acuse de recibo** antes del transcurso de un período determinado, supone que los segmentos se perdieron y los **vuelve a transmitir** (solo la parte del mensaje que se perdió, no todo el mensaje)
- En el **host receptor**, TCP se encarga de **rearmar los segmentos** del mensaje y de **pasarlos a la aplicación** (FTP - HTTP)

Estos procesos de confiabilidad **generan una sobrecarga adicional en los recursos de la red** debido a los **procesos de acuse de recibo, rastreo y retransmisión**. Para admitir estos procesos de confiabilidad, **se intercambian más datos de control entre los hosts emisores y receptores**. Esta información de control está **incluida en un encabezado TCP**.

[Mostrar Recurso 7.1.1.5](#)



## UDP

- TCP representan una **sobrecarga adicional** y pueden provocar **demoras** en la transmisión. La **imposición de sobrecarga** podría **reducir la utilidad a la aplicación e incluso ser perjudicial**. En estos casos, UDP es un protocolo de transporte mejor.
- proporciona **funciones básicas** para entregar segmentos de datos entre las aplicaciones con **muy poca sobrecarga y revisión de datos >>> protocolo de entrega de máximo esfuerzo**.
- **no hay acuse de recibo** que indique que los datos se recibieron en el destino y que informen al emisor si la entrega se produjo correctamente.

[Mostrar Recurso 7.1.1.6](#)

*Ejemplo: El proceso de UDP es similar al envío por correo de una carta simple sin registrar. El emisor de la carta no sabe si el receptor está disponible para recibir la carta ni la oficina de correos es responsable de hacer un seguimiento de la carta o de informar al emisor si esta no llega a destino.*

TCP: bases de datos, clientes web, clientes de correo electrónico, transferencia de ficheros, DNS, SNMP

UDP: streaming audio, video, voz sobre IP (VoIP), radio/tv por Internet, servicios de monitorización SNMP, DHCP, DNS

*La imagen en un streaming video se degradaría en gran medida si el dispositivo de destino tuviera que dar cuenta de los datos perdidos y demorar el stream mientras espera las retransmisiones. En este caso, es mejor producir el mejor video posible con los segmentos recibidos y prescindir de la confiabilidad.*

**Diferencias entre TCP y UDP**, es importante **comprender la manera en que cada protocolo implementa las funciones específicas de confiabilidad y la forma en que realizan el seguimiento de las comunicaciones.**

- **Protocolo de control de transmisión (TCP)**

- **establecimiento de sesiones**: negocia y establece una **conexión** (o sesión) permanente entre los dispositivos de **origen y de destino antes de reenviar tráfico**, negocian **cantidad** de tráfico que se puede reenviar en un momento determinado.
- **entrega confiable**: asegurar que cada sección de datos que envía origen **llegue** al destino.
- **reconstrucción de datos ordenada**: asegurar que estos se **rearmen en el orden correcto**.
- **control del flujo**: hosts de la red cuentan con **recursos** limitados, como memoria o ancho de banda. Cuando TCP advierte que estos recursos están **sobrecargados**, puede solicitar que la aplicación emisora **reduzca la velocidad del flujo** de datos. Puede evitar la pérdida de segmentos en la red y **evitar la necesidad de la retransmisión**.

- **Protocolo de datagramas de usuario (UDP)**, protocolo simple:

Protocolo de transporte de **máximo esfuerzo**, de **transporte liviano** que ofrece la **misma segmentación** de datos que TCP, pero **sin la confiabilidad y el control del flujo**.

- **sin conexión**: no establece conexión entre los hosts antes de que se puedan enviar y recibir datos.
- **entrega no confiable**: no proporciona servicios para asegurar que los datos se entreguen con confianza, **no** cuenta con procesos que hagan que el **emisor vuelva a transmitir** los datos que se pierden o se dañan.
- **reconstrucción de datos no ordenada**: no proporciona ningún mecanismo para rearmar los datos en su **secuencia original**, se entregan a la aplicación en el orden en que **llegan**.
- **sin control del flujo**: **no** cuenta con **mecanismos para controlar la cantidad de datos** que transmite el dispositivo de origen para **evitar la saturación** del dispositivo de destino. El origen envía los datos. Si los recursos en el host de destino se sobrecargan, es probable que dicho **host descarte los datos enviados** hasta que los recursos estén disponibles. No hay un mecanismo para la retransmisión automática de datos descartados.

UDP y TCP deben hacer un seguimiento de las diversas aplicaciones que se comunican. Para diferenciar los segmentos y datagramas para cada aplicación, para ello cuentan con campos de encabezado que pueden identificar de manera **exclusiva** estas aplicaciones. Estos identificadores únicos son números de puertos.



El término *puerto* se utiliza en Internet, su termino genérico es el de *Punto de Acceso al Servicio de Transporte*, cuyas siglas en inglés son **TSAP**.

## Direccionamiento de puertos TCP y UDP

En el **encabezado** de cada segmento habrá **un puerto origen y otro destino**.

- **El número de puerto de origen:** es el **número para la comunicación** asociado con la aplicación que origina la comunicación en el host local.
- **El número de puerto de destino:** es el **número para la comunicación** relacionada con la aplicación de destino en el host remoto.

Cuando se **envía un mensaje utilizando TCP o UDP**, los **protocolos y servicios** solicitados se **identifican con un número de puerto**.

Un puerto es un **identificador numérico** de cada segmento, que se utiliza para realizar un **seguimiento de conversaciones específicas y de servicios de destino solicitados**. Cada mensaje que envía un host contiene un puerto de origen y un puerto de destino.

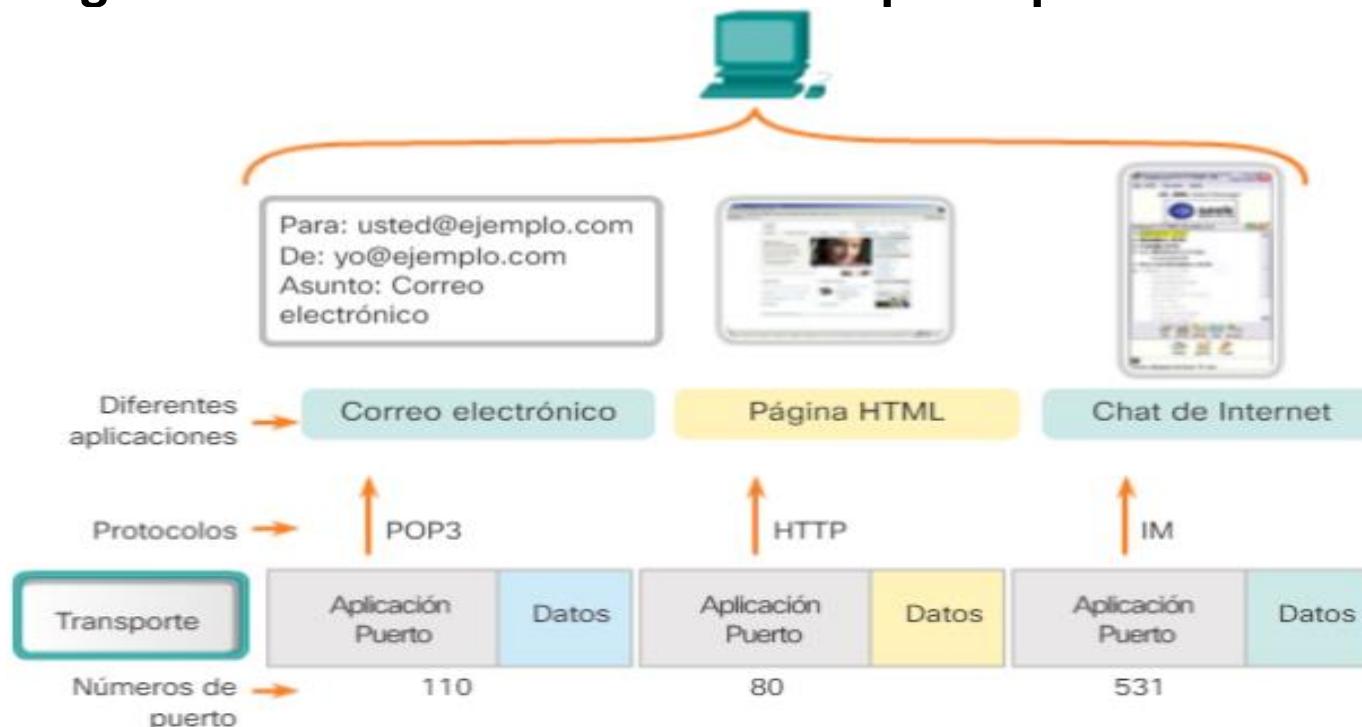
*Es interesante que leas algo más sobre los protocolos más importantes de este nivel, por lo que te proponemos los siguientes enlaces.*

[http://es.wikipedia.org/wiki/Transmission\\_Control\\_Protocol](http://es.wikipedia.org/wiki/Transmission_Control_Protocol)

[http://es.wikipedia.org/wiki/User\\_Datagram\\_Protocol](http://es.wikipedia.org/wiki/User_Datagram_Protocol)

## Ejemplo:

- Puerto de **destino**: el **cliente** coloca un número de puerto de destino en el segmento para informar al servidor de destino el servicio solicitado. Cuando un **cliente especifica el puerto 80** en el puerto de destino, el servidor que recibe el mensaje sabe que se **solicitan servicios Web**. Un servidor puede **ofrecer más de un servicio simultáneamente**. Puede ofrecer servicios Web en el puerto 80 al mismo tiempo que ofrece el establecimiento de una conexión FTP en el puerto 21.
- Puerto de **origen**: el número de puerto de origen es generado de manera **aleatoria** por el **dispositivo emisor** para **identificar una conversación entre dos dispositivos**. Esto permite establecer varias **conversaciones simultáneamente**. Puede enviar varias solicitudes de servicio HTTP a un servidor Web al mismo tiempo. El **seguimiento de las conversaciones por separado se basa en los puertos de origen**.



Los puertos de origen y de destino se colocan **dentro del segmento**. Los segmentos se encapsulan **dentro de un paquete IP**. El paquete IP contiene la **dirección IP de origen y de destino**.

La **combinación de las direcciones IP de origen y de destino y de los números de puerto de origen y de destino** se conoce como "**socket**".

- El socket se utiliza para **identificar el servidor y el servicio que solicita el cliente**. Los sockets identifican las comunicaciones entre host y servidor.

*Ejemplo: un socket cliente puede ser parecido a 192.168.1.5:1099, donde 1099 representa el número de puerto de origen, un socket servidor (Web) podría ser: 192.168.1.7:80. Juntos, estos dos sockets se combinan para formar un par de sockets: 192.168.1.5:1099, 192.168.1.7:80*

Con la creación de sockets, se **conocen los extremos de la comunicación**, de modo que los **datos puedan moverse desde una aplicación en un host hacia una aplicación en otro host**.

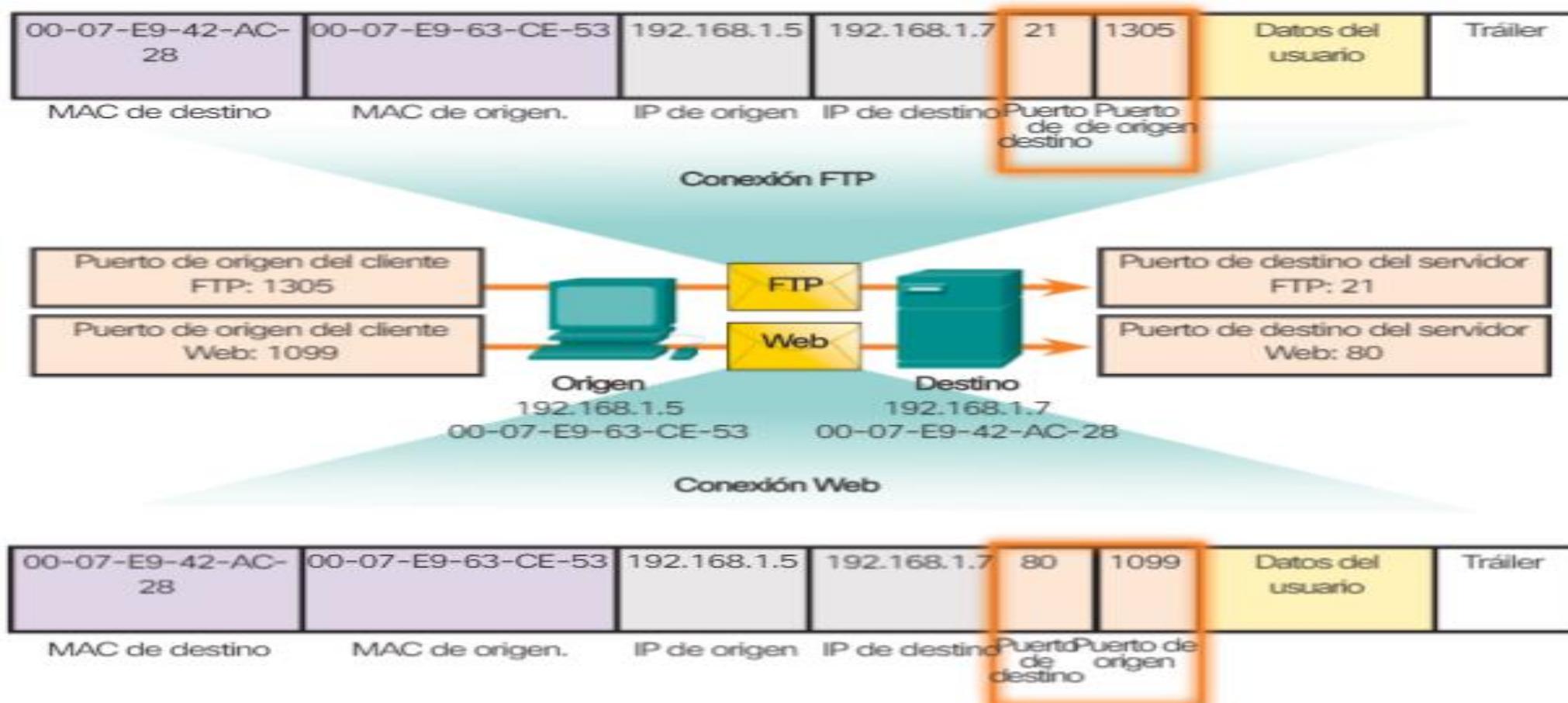
Los **sockets** permiten que:

- los **procesos múltiples** que se ejecutan en un cliente se **distingan** entre sí
- la **diferenciación de múltiples conexiones a un proceso de servidor**.

**El puerto de origen** de la solicitud de un cliente se genera de manera aleatoria.

El número de puerto **actúa como dirección de retorno** para la aplicación que realiza la solicitud. La capa de transporte hace un **seguimiento de este puerto** y de la **aplicación que generó la solicitud** de manera que cuando se devuelva una respuesta, esta se envíe 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.

[Mostrar recurso 7.2.1.2](#)



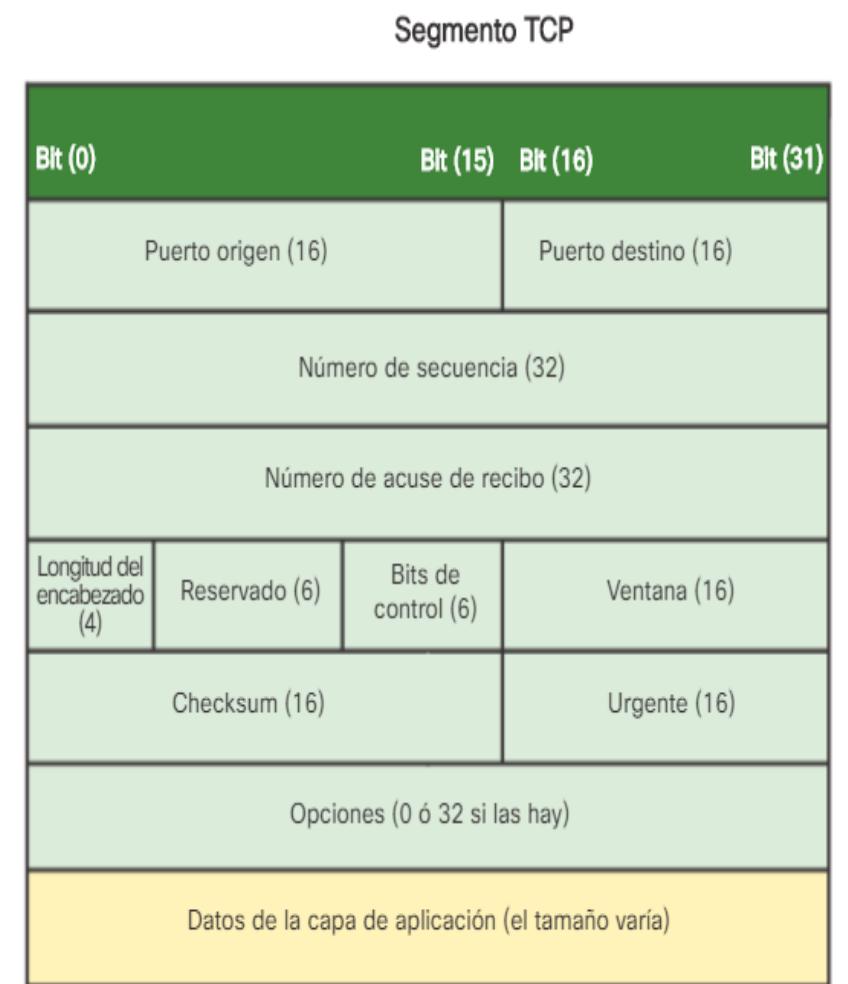
## Algunos puertos conocidos son:

- 20 ftp-data Puerto de datos FTP
- 21 ftp Puerto del Protocolo de transferencia de archivos (FTP)
- 22 ssh Servicio de shell seguro (SSH)
- 23 telnet El servicio Telnet
- 25 smtp Protocolo simple de transferencia de correo (SMTP)
- 53 domain Servicios de nombres de dominio DNS (tales como BIND)
- 67/68 bootp-dhcp **Servicios del Protocolo Bootstrap o inicio (BOOTP), servicios (DHCP)**
- 69 tftp Protocolo de transferencia de archivos triviales (TFTP)
- 79 finger Servicio Finger para información de contacto de usuarios
- 80 http **Protocolo de transferencia de hipertexto (HTTP) para los servicios WWW**
- 88 kerberos Sistema de autenticación de redes Kerberos
- 107 rtelnet Telnet remoto
- 110 pop3 **Protocolo Post Office versión 3**
- 115 sftp Servicios del protocolo de transferencia de archivos seguros (SFTP)

- 123 ntp Protocolo de tiempo de red (NTP)
- 143 imap Protocolo de acceso a mensajes de Internet (IMAP)
- 161 snmp Protocolo simple de administración de redes (SNMP)
- 179 bgp Border Gateway Protocol
- 389 ldap Protocolo Lightweight de acceso a directorios (LDAP)
- 443 https Protocolo de transferencia de hipertexto seguro (HTTP)
- 546 dhcipv6-client Cliente DHCP, Protocolo de configuración dinámica de host, versión 6
- 1812 radius Servicios de contabilidad y autenticación de marcado Radius
- 2049 nfs Sistema de archivos de red (NFS)
- 465 smtps Protocolo simple de transferencia de correo sobre Capas Segura (SMTPS)
- 901 swat Herramienta de administración Web de Samba (SWAT)
- 5432 postgres Base de datos PostgreSQL
- 8080 webcache Servicio de caché del World Wide Web (WWW)
- 9100 jetdirect Servicio de impresión de redes Hewlett-Packard (HP) JetDirect
- 5400 VNC protocolo de escritorio remoto (usado sobre HTTP)
- 3306 MySQL sistema de gestión de bases de datos
- 4662 eMule (aplicación de compartición de ficheros)
- 5222 Jabber/XMPP conexión de cliente
- 6881 BitTorrent puerto por defecto
- 10000 Webmin (Administración remota web)

TCP **genera sobrecarga adicional**, cada segmento TCP tiene 20 bytes de sobrecarga en el **encabezado** que encapsula los datos de la capa de aplicación. Un segmento UDP solo tiene 8 bytes de sobrecarga. La sobrecarga adicional incluye:

- **Número de secuencia** (32 bits): para rearmar datos.
- **Número de acuse de recibo** (32 bits): indica los datos que se recibieron.
- **Bits de control** (6 bits): indican el propósito y la función del segmento TCP.
- **Checksum** (16 bits): se utiliza para la verificación de errores en el encabezado y los datos del segmento.
- **Urgente** (16 bits): indica si la información es urgente.



## Existen diferentes tipos de números de puerto

- **Puertos bien conocidos:**
  - números del **0 al 1023**
  - se reservan para **servicios y aplicaciones** como HTTP, protocolo de acceso a mensajes de Internet (IMAP) o protocolo simple de transferencia de correo (SMTP) y Telnet.
  - las aplicaciones cliente se pueden **programar para solicitar una conexión a ese puerto** en particular y el servicio relacionado (son conocidos)
- **Puertos registrados :**
  - números del **1024 al 49151**
  - se asignan a **procesos o aplicaciones del usuario**
  - son aplicaciones individuales que el usuario elige instalar en lugar de aplicaciones comunes, aplicaciones no estándares
- **Puertos dinámicos o privados:**
  - números **49152 a 65535** ( $2^{16}$ )
  - puertos **efímeros**
  - se asignan de forma dinámica a las aplicaciones **cliente** cuando el cliente **inicia una conexión a un servicio**, para **identificar** la aplicación cliente durante la comunicación

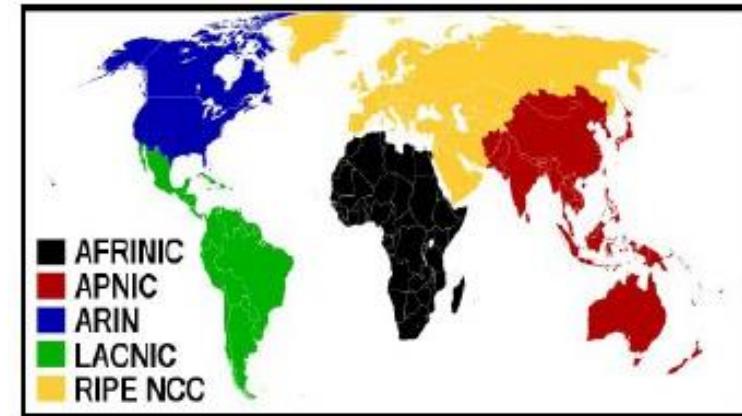
- **IANA:**

Actividad 7.1.2.11

Internet Assigned Numbers Authority, es la Agencia de **Asignación de Números de Internet**. Era el antiguo registro central de los protocolos Internet, como puertos, números de protocolo y empresa, opciones y códigos. Fue sustituido en 1998 por **ICANN** (Internet Corporation for Assigned Names and Numbers). Existen 5 Regional Internet Registry (**RIR**)

Para conocer más sobre la función de este organismo, te recomiendo el siguiente enlace:

<https://www.icann.org/es/system/files/files/iana-functions-18dec15-es.pdf>



La mayor parte de los servicios usan TCP o UDP pero **algunos pueden comunicar con ambos**.

Se reserva habitualmente ambos números TCP y UDP para el mismo servicio.

El RFC que se encarga de documentarlo es: **RFC 6335**.

<https://tools.ietf.org/html/rfc6335>

Para conocer los puertos relacionados con cada una de las aplicaciones, te recomendamos el siguiente enlace.

<https://www.iana.org/assignments/service-names-port-numbers/service-names-port-numbers.xhtml>

**Netstat** (network statistics – Estadística de red) es una herramienta de línea de comando que incluyen los Sistemas Operativos Windows y Linux y que, con la que obtendremos **información valiosa a nivel de red**.

[Mostrar recurso 7.1.2.9](#)

Indica el **protocolo** que se está usando, la **dirección** y el número de **puerto locales**, la **dirección** y el número de **puerto externos** y el **estado** de la conexión.

Con netstat podemos conocer: **netstat**

- **todas las conexiones TCP activas en la máquina**
- **listar todos los puertos UDP y TCP abiertos en la máquina.**

Opciones:

**-e:** visualizar las estadísticas de Ethernet, tanto de paquetes enviados como recibidos.

Estadísticas de interfaz		
	Recibidos	Enviados
Bytes	1570389435	89621971
Paquetes de unidifusión	1189356	453075
Paquetes no de unidifusión	371	19198
Descartados	0	0
Errores	0	0
Protocolos desconocidos	0	

Información del estado de las conexiones	
NETSTAT devuelve una serie de parámetros que indican el estado en que se encuentran las conexiones, son los siguientes:	
LISTENING:	El puerto está abierto escuchando en espera de una conexión.
ESTABLISHED:	La conexión ha sido establecida.
CLOSE_WAIT:	La conexión sigue abierta, pero el otro extremo nos comunica que no se continuará enviando información.
TIME_WAIT:	La conexión ha sido cerrada, pero no se elimina de la tabla de conexión por si hay algo pendiente de recibir.
LAST_ACK:	La conexión se está cerrando.
CLOSED:	La conexión ha sido cerrada completamente.

```
Microsoft Windows [Versión 10.0.17134.523]
(c) 2018 Microsoft Corporation. Todos los derechos reservados.

C:\Users\Alfonso>netstat
Símbolo del sistema
Microsoft Windows [Versión 10.0.17134.523]
(c) 2018 Microsoft Corporation. Todos los derechos reservados.

C:\Users\Alfonso>netstat
Conexiones activas

Proto  Dirección local          Dirección remota        Estado
TCP    127.0.0.1:62464          DESKTOP-AGJ4THS:62465 ESTABLISHED
TCP    127.0.0.1:62465          DESKTOP-AGJ4THS:62464 ESTABLISHED
TCP    192.168.1.132:56717     152.199.19.161:https LAST_ACK
TCP    192.168.1.132:56836     a2-17-133-7:https ESTABLISHED
TCP    192.168.1.132:56837     a2-17-133-7:https ESTABLISHED
TCP    192.168.1.132:56838     a2-17-133-7:https ESTABLISHED
TCP    192.168.1.132:56839     a2-17-133-7:https ESTABLISHED
TCP    192.168.1.132:56840     a2-17-133-7:https ESTABLISHED
TCP    192.168.1.132:56841     a2-20-90-210:http ESTABLISHED
TCP    192.168.1.132:56842     a2-20-90-210:http ESTABLISHED
TCP    192.168.1.132:56843     a2-20-90-210:http ESTABLISHED
TCP    192.168.1.132:56844     a2-20-90-210:http ESTABLISHED
TCP    192.168.1.132:56845     a2-20-90-210:http ESTABLISHED
TCP    192.168.1.132:56846     a2-20-90-210:http ESTABLISHED
TCP    192.168.1.132:56851     40.67.255.199:https ESTABLISHED
TCP    192.168.1.132:56855     wn-in-f188:5228 ESTABLISHED
TCP    192.168.1.132:56856     mad07s09-in-f3:https ESTABLISHED
TCP    192.168.1.132:56857     mad07s09-in-f14:https ESTABLISHED
TCP    192.168.1.132:56858     mad08s06-in-f3:https ESTABLISHED
TCP    192.168.1.132:56859     ws-in-f109:imaps ESTABLISHED
TCP    192.168.1.132:56860     ws-in-f109:imaps ESTABLISHED
TCP    192.168.1.132:56861     mad08s06-in-f10:https ESTABLISHED
```

**-a:** mostrar las conexiones y los puertos de escucha activos

**-n:** visualizar las direcciones y números de puerto en forma numérica

**-p [Protocolo]:** información solicitada sobre el protocolo que hemos definido, por ejemplo, para ver información de TCP

Conexiones activas				
Proto	Dirección local	Dirección remota	Estado	
TCP	127.0.0.1:57851	DESKTOP-AG414THS:57852	ESTABLISHED	
TCP	127.0.0.1:57052	DESKTOP-AG414THS:57051	ESTABLISHED	
TCP	192.168.1.132:56836	a2-17-133-7:https	ESTABLISHED	
TCP	192.168.1.132:56837	a2-17-133-7:https	ESTABLISHED	
TCP	192.168.1.132:56838	a2-17-133-7:https	ESTABLISHED	
TCP	192.168.1.132:56839	a2-17-133-7:https	ESTABLISHED	
TCP	192.168.1.132:56840	a2-17-133-7:https	ESTABLISHED	
TCP	192.168.1.132:56841	a2-20-96-210:http	ESTABLISHED	
TCP	192.168.1.132:56842	a2-20-96-210:http	ESTABLISHED	
TCP	192.168.1.132:56843	a2-20-96-210:http	ESTABLISHED	
TCP	192.168.1.132:56844	a2-20-96-210:http	ESTABLISHED	
TCP	192.168.1.132:56845	a2-20-96-210:http	ESTABLISHED	
TCP	192.168.1.132:56846	a2-20-96-210:http	ESTABLISHED	
TCP	192.168.1.132:56851	a0_61_255_199:https	ESTABLISHED	
TCP	192.168.1.132:56960	wm-in-188-5223:https	ESTABLISHED	
TCP	192.168.1.132:57024	mad07@09-in-f44:https	ESTABLISHED	
TCP	192.168.1.132:57054	wb-in-100e:maps	ESTABLISHED	
TCP	192.168.1.132:57068	wh-in-100e:maps	ESTABLISHED	
TCP	192.168.1.132:57136	wo-in-100e:maps	ESTABLISHED	
TCP	192.168.1.132:57137	mad08@06-in-f10:https	TIME_WAIT	
TCP	192.168.1.132:57139	arnn@2006-in-f16:https	ESTABLISHED	
TCP	192.168.1.132:57140	mad07@09-in-f3:https	ESTABLISHED	
TCP	192.168.1.132:57141	mad07@09-in-f44:https	ESTABLISHED	
TCP	192.168.1.132:57142	mad08@04-in-f3:https	ESTABLISHED	
TCP	192.168.1.132:57143	72:ftp	ESTABLISHED	
TCP	192.168.1.132:57144	72:40234	ESTABLISHED	

**-o:** ver el número de proceso (PID) asignado a cada conexión

-r: tendremos acceso a la tabla de enrutamiento del sistema

```

C:\Users\Alfonso\netstat -r
Tráfico de interfaces
11...00:0c:29:1d:fa:a7 ... Realtek PCIe GBE Family Controller
10...00:0c:29:1d:fa:a8 ... VirtualBox Host-Only Ethernet Adapter
18...bb:6b:fc:9a:dc:c4 ... Microsoft Wi-Fi Direct Virtual Adapter
6...bb:6b:fc:9a:dc:39 ... Microsoft Wi-Fi Direct Virtual Adapter #2
17...bb:6b:fc:9a:dc:30 ... Intel PRO/1000 MT Desktop-NIC 3165
4...00:0c:29:3d:cd:01 ... Bluetooth Device (Personal Area Network)
1...00:0c:29:3d:cd:01 ... Software Loopback Interface 1

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         192.168.1.1       192.168.1.132   40
127.0.0.0         255.0.0.0       En vinculo        En vinculo      331
127.0.0.1         255.255.255.255 En vinculo        En vinculo      331
127.255.255.255 255.255.255.255 En vinculo        En vinculo      331
192.168.1.0       255.255.255.0   En vinculo        En vinculo      296
192.168.1.132    255.255.255.0   En vinculo        En vinculo      296
192.168.1.132    255.255.255.255 En vinculo        En vinculo      296
192.168.56.0      255.255.255.0   En vinculo        En vinculo      281
192.168.56.1      255.255.255.0   En vinculo        En vinculo      281
192.168.56.255    255.255.255.255 En vinculo        En vinculo      281
224.0.0.0          240.0.0.0       En vinculo        En vinculo      331
224.0.0.0          240.0.0.0       En vinculo        En vinculo      281
224.0.0.0          240.0.0.0       En vinculo        En vinculo      281
224.0.0.0          240.0.0.0       En vinculo        En vinculo      281
255.255.255.255  255.255.255.255 En vinculo        En vinculo      331
255.255.255.255  255.255.255.255 En vinculo        En vinculo      281
255.255.255.255  255.255.255.255 En vinculo        En vinculo      281

```

-s: estadísticas detalladas de cada protocolo

```
C:\Users\Alfonso>netstat -n
```

## Conexiones activas

Proto	Dirección local	Dirección remota	Estado
TCP	127.0.0.1:57051	127.0.0.1:57052	ESTABLISHED
TCP	127.0.0.1:57052	127.0.0.1:57051	ESTABLISHED
TCP	192.168.1.132:56836	2.17.133.7:443	ESTABLISHED
TCP	192.168.1.132:56837	2.17.133.7:443	ESTABLISHED
TCP	192.168.1.132:56838	2.17.133.7:443	ESTABLISHED
TCP	192.168.1.132:56839	2.17.133.7:443	ESTABLISHED
TCP	192.168.1.132:56840	2.17.133.7:443	ESTABLISHED
TCP	192.168.1.132:56841	2.20.90.210:80	ESTABLISHED
TCP	192.168.1.132:56842	2.20.90.210:80	ESTABLISHED
TCP	192.168.1.132:56843	2.20.90.210:80	ESTABLISHED
TCP	192.168.1.132:56844	2.20.90.210:80	ESTABLISHED
TCP	192.168.1.132:56845	2.20.90.210:80	ESTABLISHED
TCP	192.168.1.132:56846	2.20.90.210:80	ESTABLISHED
TCP	192.168.1.132:56851	40.67.255.199:443	ESTABLISHED

```
C:\Users\Alfonso>netstat -o
```

## Conexiones activas

Proto	Dirección local	Dirección remota	Estado	PID
TCP	127.0.0.1:57051	DESKTOP-AGJ4THS:57052	ESTABLISHED	14168
TCP	127.0.0.1:57052	DESKTOP-AGJ4THS:57051	ESTABLISHED	14168
TCP	192.168.1.132:56836	a2-17-133-7:https	ESTABLISHED	10300
TCP	192.168.1.132:56837	a2-17-133-7:https	ESTABLISHED	10300
TCP	192.168.1.132:56838	a2-17-133-7:https	ESTABLISHED	10300
TCP	192.168.1.132:56839	a2-17-133-7:https	ESTABLISHED	10300
TCP	192.168.1.132:56840	a2-17-133-7:https	ESTABLISHED	10300
TCP	192.168.1.132:56841	a2-20-90-210:http	ESTABLISHED	10300
TCP	192.168.1.132:56842	a2-20-90-210:http	ESTABLISHED	10300
TCP	192.168.1.132:56843	a2-20-90-210:http	ESTABLISHED	10300
TCP	192.168.1.132:56844	a2-20-90-210:http	ESTABLISHED	10300
TCP	192.168.1.132:56845	a2-20-90-210:http	ESTABLISHED	10300
TCP	192.168.1.132:56846	a2-20-90-210:http	ESTABLISHED	10300
TCP	192.168.1.132:56851	40.67.255.199:https	ESTABLISHED	3976
TCP	192.168.1.132:56960	wm-in-f188:5228	ESTABLISHED	4540
TCP	192.168.1.132:57054	wb-in-f109:imaps	ESTABLISHED	14168
TCP	192.168.1.132:57136	wo-in-f108:imaps	ESTABLISHED	14168

Estadísticas de TCP para IPv4

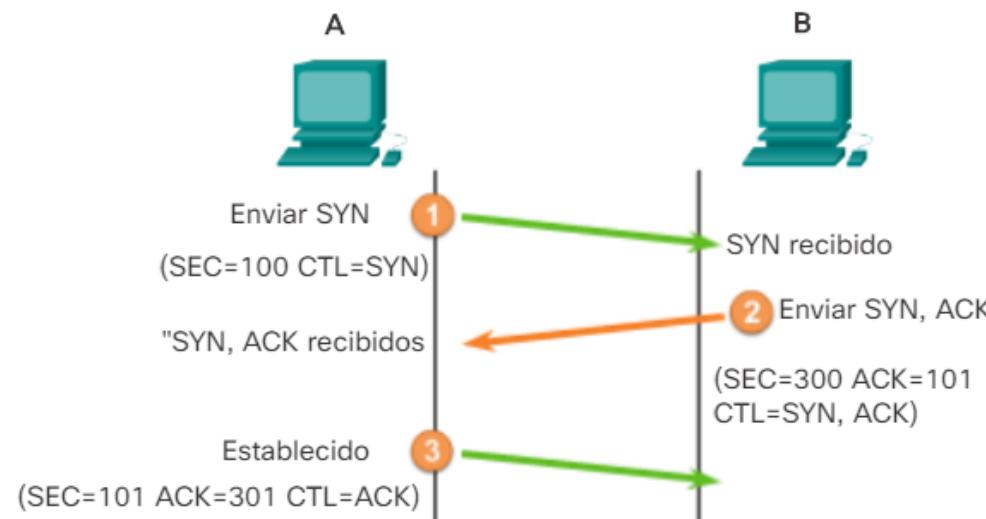
Activos abiertos	= 29681
Pasivos abiertos	= 952
Intentos de conexión erróneos	= 553
Conexiones restablecidas	= 3617
Conexiones actuales	= 26
Segmentos recibidos	= 3882908
Segmentos enviados	= 1803740
Segmentos retransmitidos	= 9733

## Establecimiento y finalización de la conexión TCP.

Cuando dos hosts se comunican utilizando TCP, se establece una conexión **antes** de que puedan intercambiarse los datos. Cuando se completa la comunicación, se **cierran** las sesiones y finaliza.

*En algunas culturas, cuando dos personas se conocen, generalmente se saludan dándose la mano. Ambas culturas entienden el acto de darse la mano como señal de un saludo amigable y a partir de ese momento puede comenzar la comunicación. Las conexiones en la red son similares.*

- El primer enlace **solicita la sincronización**.
- El segundo enlace **acusa recibo de la solicitud de sincronización inicial y sincroniza los parámetros de conexión en la dirección opuesta**.
- El tercer segmento de enlace es un **acuse de recibo que se utiliza para informarle al destino que ambos lados están de acuerdo** en que se estableció una conexión.



CTL = Bits de control establecidos en 1 en el encabezado TCP

A envía una respuesta ACK a B.

Los hosts hacen un seguimiento de cada segmento de datos dentro de una sesión e intercambian información sobre qué datos se reciben mediante la información del **encabezado TCP**.

Para establecer la conexión los hosts realizan un **protocolo de enlace de tres vías**. Los **bits de control** en el encabezado TCP indican el progreso y estado de la conexión:

- Paso 1. El cliente de **origen** solicita una **sesión de comunicación** de cliente a servidor con el servidor.
- Paso 2. El **servidor** acusa **recibo** de la sesión de comunicación de cliente a servidor y **solicita una sesión de comunicación de servidor a cliente**.
- Paso 3. El **cliente de origen** acusa **recibo de la sesión de comunicación** de servidor a cliente.

Observa los diversos valores que intercambian ambos hosts. Dentro del encabezado del segmento TCP, existen seis campos de 1 bit que contienen **información de control** utilizada para gestionar los procesos de TCP, los más significativos son:

- **ACK**: campo de acuse de **recibo** importante
- **SYN**: sincronizar números de secuencia
- **FIN**: no hay más datos del emisor

The screenshot shows a TCP segment from a Wireshark capture. The segment details are as follows:

- Transmission Control Protocol, Src Port: http (80), Dst Port: 49523 (49523), Seq: 0, Ack: 1, Len: 0
- Source port: http (80)
- Destination port: 49523 (49523)
- [Stream index: 2]
- Sequence number: 0 (relative sequence number)
- Acknowledgment number: 1 (relative ack number)
- Header length: 32 bytes
- Flags: 0x012 (SYN, ACK)
  - 000. .... .... = Reserved: Not set
  - ...0 .... .... = Nonce: Not set
  - .... 0.... .... = Congestion Window Reduced (CWR): Not set
  - .... .0.... .... = ECN-Echo: Not set
  - .... ..0.... .... = Urgent: Not set
  - .... ..1.... .... = Acknowledgment: Set
  - .... ....0.... .... = Push: Not set
  - .... ....0.... .... = Reset: Not set
  - .... ..1.... .... = Syn: Set
  - .... ....0.... .... = Fin: Not set

[Mostrar Recurso 7.2.1.7](#)

Actividad 7.2.1.9 Proceso Conexión y Finalización TCP

Actividad 7.2.1.8 Using Wireshark to Observe the TCP

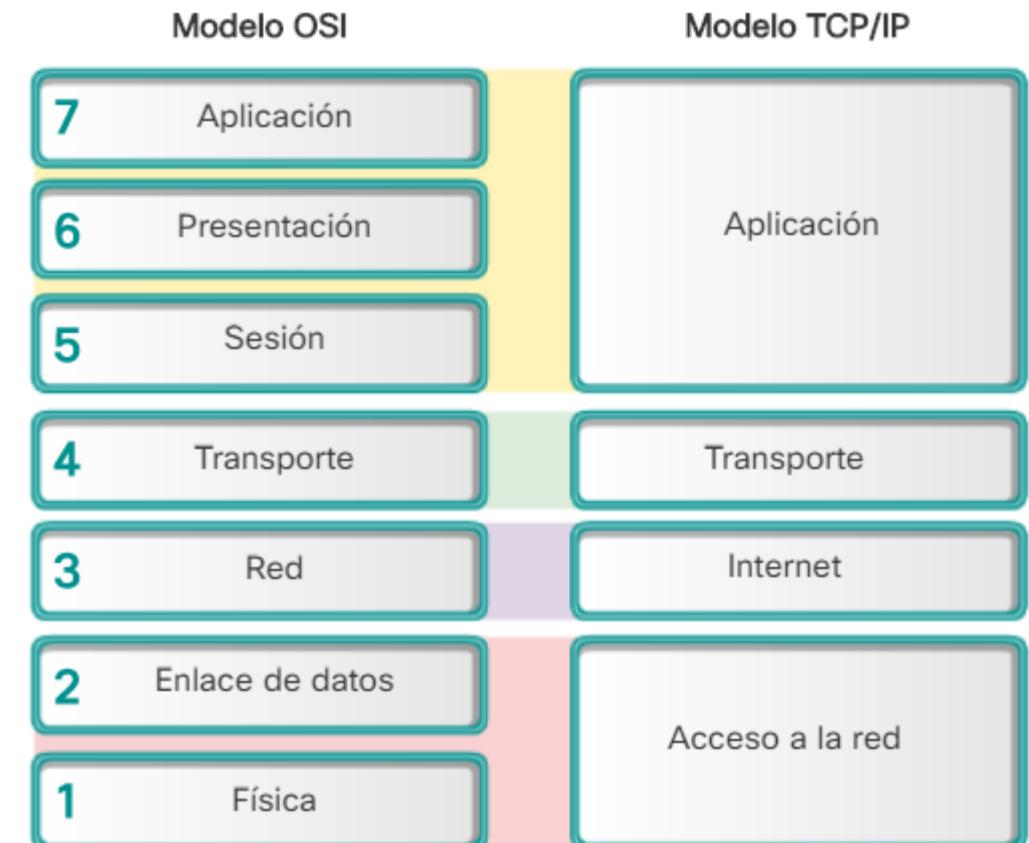
# Capa4 o Nivel de Aplicación.

El nivel aplicación contiene los **programas de usuario: aplicaciones** que hace que nuestro ordenador pueda crear textos, chatear, leer correo, visitar páginas web, trasferir ficheros, etc. Incluyen los protocolos de alto nivel que utilizan los programas para comunicarse.

En la arquitectura TCP/IP este nivel incluye a los **niveles de sesión, presentación y aplicación** del modelo OSI.

La **información pasa de una capa a otra:**

de la capa de **aplicación** en el host de transmisión desciende por la jerarquía hacia la capa física y luego por el **canal** de comunicaciones hacia el host de destino, donde la información asciende por la jerarquía y termina en la capa de **aplicación**.



Para que las comunicaciones se lleven a cabo correctamente, los **protocolos de capa de aplicación** que se implementaron en los hosts de **origen** y de **destino** deben ser **compatibles**. Los protocolos de aplicación **especifican el formato y la información de control** necesarios para las funciones de comunicación comunes de Internet.

Algunos de los protocolos más importantes de esta capa son:

- **Sistema de nombres de dominios (DNS):** resuelve nombres de Internet en direcciones IP.  
*Cuando nosotros escribimos una dirección web > en realidad estamos conectando con una dirección IP. Un protocolo realiza la equivalencia.*
- **Protocolo simple de transferencia de correo (SMTP):** transfiere mensajes y archivos adjuntos de correo electrónico. Está basado en el concepto cliente-servidor, donde un cliente envía un mensaje a uno o varios servidores.
- **Protocolo de configuración dinámica de host (DHCP):** para asignar una dirección IP, máscara de subred, gateway predeterminado y servidor DNS a un host.
- **Protocolo de transferencia de archivos (FTP):** transferencia de archivos interactiva entre sistemas.
- **Protocolo trivial de transferencia de archivos (TFTP):** transferencia de archivos sin conexión.

- **Protocolo de transferencia de hipertexto (HTTP):** transfiere archivos que conforman las páginas Web de la World Wide Web. Sigue el esquema petición-respuesta entre cliente/servidor. Tiene una versión segura que es el **HTTPS**. Define la **sintaxis** y la **semántica** que utilizan los clientes, servidores para comunicarse.



- **Telnet:** para proporcionar acceso remoto a servidores y dispositivos de red.
- **SSH:** proporcionar acceso remoto a servidores y dispositivos de red con encriptación.
- **SNMP:** protocolo de administración de redes, permite monitorizar y controlar los dispositivos de red, y de administrar configuraciones y seguridad.
- **Protocolo bootstrap (BOOTP):** es un precursor del protocolo DHCP, se utiliza para obtener información de la dirección IP durante el arranque.
- **Protocolo de oficina de correos (POP):** lo utilizan los clientes de correo electrónico para recuperar el correo electrónico de un servidor remoto.
- **Protocolo de acceso a mensajes de Internet (IMAP):** este es otro protocolo que se utiliza para recuperar correo electrónico.

- **Protocolo de transferencia de hipertexto y lenguaje de marcado de hipertexto. HTTP.**

Cuando se escribe una dirección Web en un explorador, se establece una **conexión con el servicio Web** que se ejecuta en el servidor, mediante el protocolo HTTP. Los nombres que la mayoría de las personas asocia con las direcciones Web son URL.

*Ejemplo: <http://www.cisco.com/index.html> es un ejemplo de un URL que se refiere a un recurso específico, una página Web llamada index.html en un servidor identificado como cisco.com.*

Los **exploradores Web** son aplicaciones **cliente** que utiliza un PC para **conectarse** a la WWW y acceder a **recursos** almacenados en un servidor Web.

El **servidor Web** funciona como un servicio básico que responde con el recurso solicitado por el cliente.

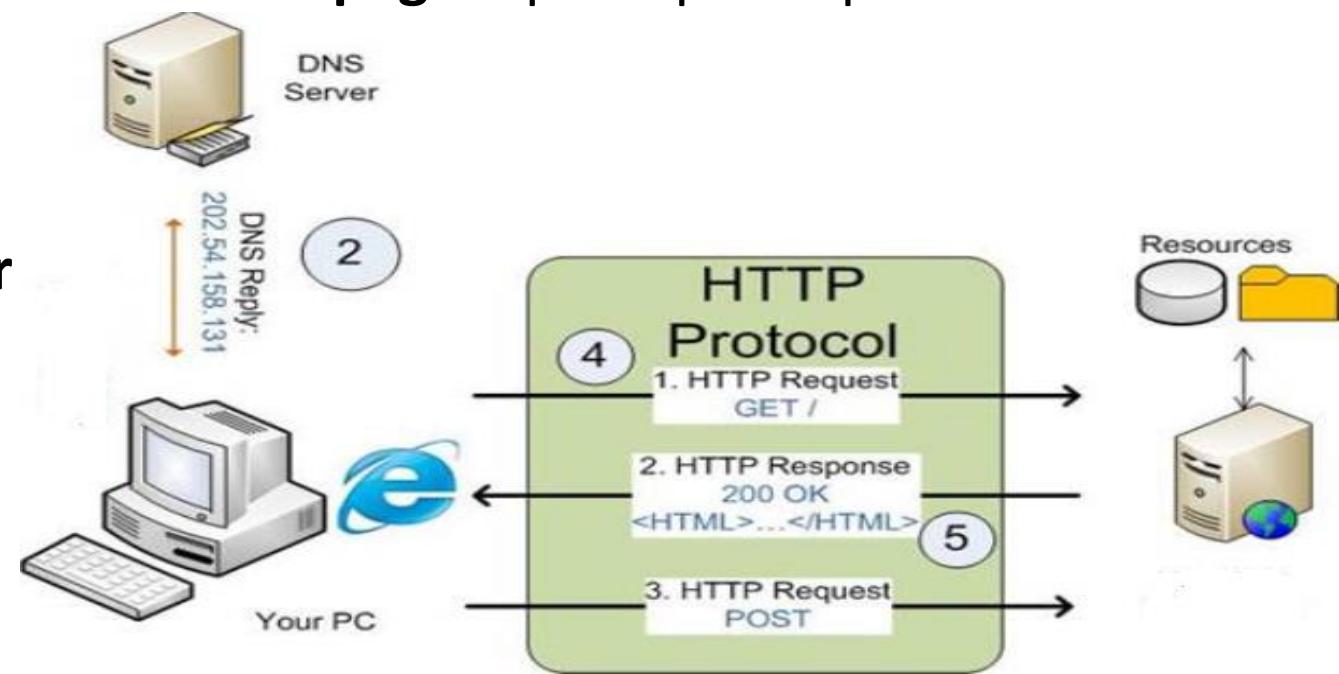
El cliente al recibir los datos mediante el explorador(cliente) interpreta los datos y los presenta al usuario.

# Análisis de cómo se abre una página Web en un explorador.

- El explorador interpreta las tres **partes del URL**
  1. **http** (el **protocolo** o esquema)
  2. **www.cisco.com** (el nombre del **servidor**)
  3. **index.html** (el nombre de archivo específico solicitado o **recurso**)
- El explorador verifica con un servidor de nombre (DNS) para **convertir** www.cisco.com en una **dirección numérica** que utiliza para conectarse al servidor.
- El explorador envía una **solicitud GET** al servidor y **solicita el archivo index.html**
- El servidor **envía el código HTML** para esta página Web al explorador
- El explorador **descifra el código HTML y da formato a la página** para que se pueda visualizar en la ventana del explorador.

[Mostrar Recurso 10.2.1.2](#)

Los mensajes **POST** y **PUT** se utilizan para **subir datos al servidor Web** cuando el usuario introduce datos en un **formulario** que está integrado en una página Web.

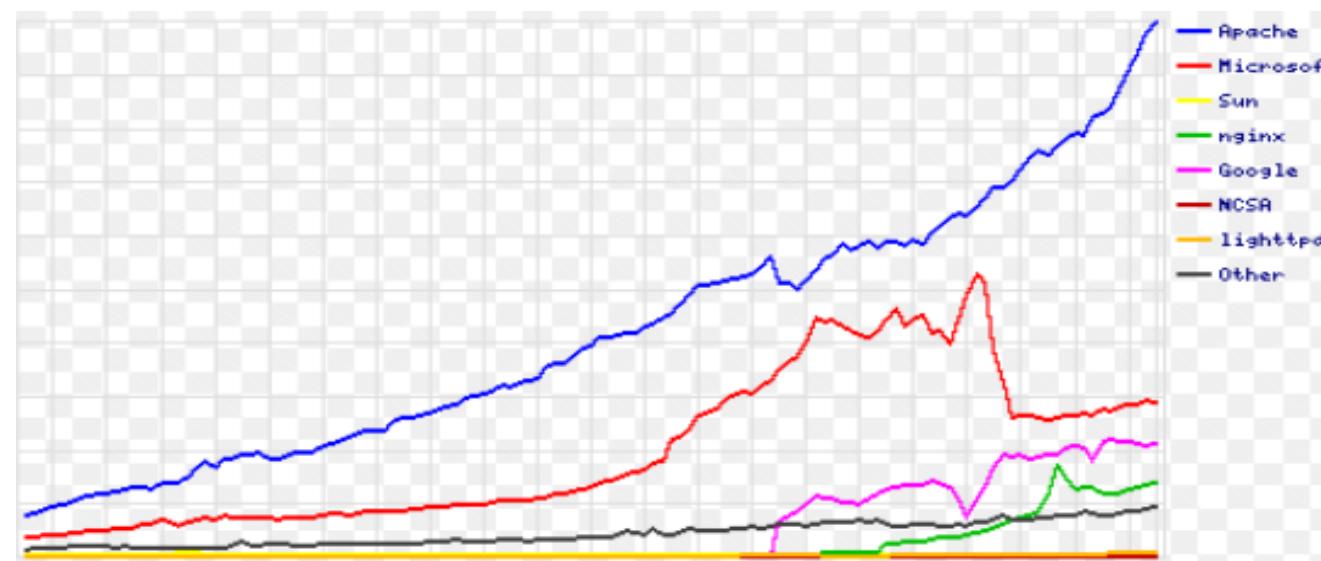


El **HTTPS** puede utilizar **autenticación y encriptación** para asegurar los datos mientras viajan entre el cliente y el servidor.

- **especifica reglas adicionales** para pasar datos entre la capa aplicación y capa de transporte
- **utiliza el mismo proceso de solicitud del cliente-respuesta** del servidor que HTTP
- el stream de datos se **encripta** con capa de sockets seguros (SSL) antes de transportarse
- **crea una carga y un tiempo de procesamiento adicionales** en el servidor debido a la encriptación y el descifrado

Existen varios servidores Web tanto para sistemas GNU/Linux como para sistemas Windows.

**Apache** es el servidor Web **más utilizado en Internet** muy por encima del resto de competidores.



- **SMTP, POP e IMAP**

El correo electrónico **revolucionó** la forma en que las personas se comunican gracias a su **sencillez y velocidad**. Para ejecutar el correo electrónico en un PC o en otro dispositivo final, este **requiere varios servicios y aplicaciones**.

Es un método para **enviar, almacenar y recuperar mensajes electrónicos** a través de una red. Los mensajes de correo electrónico se guardan en **bases de datos** en **servidores de correo**.

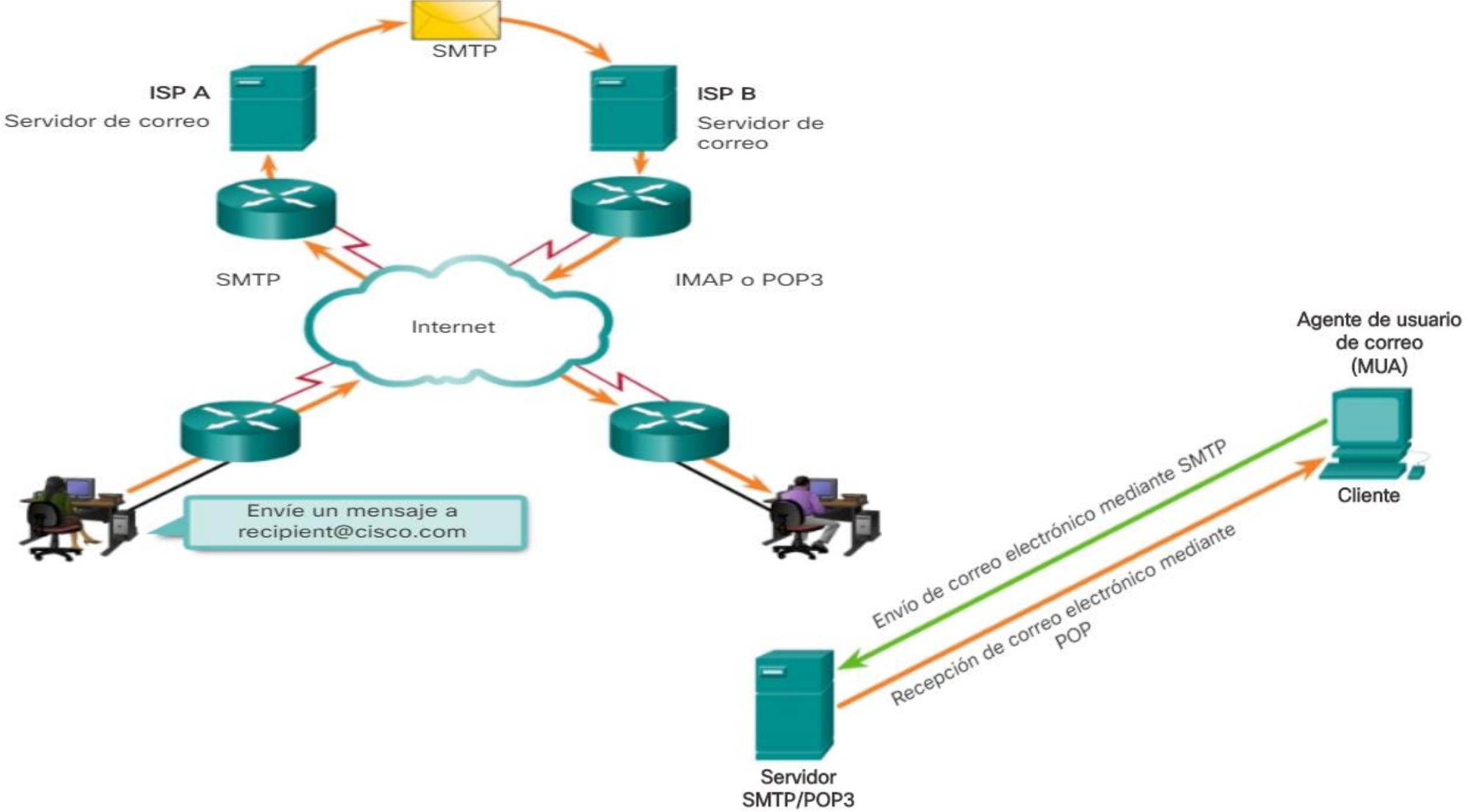
La **funcionalidad** que todo usuario espera de este sistema es:

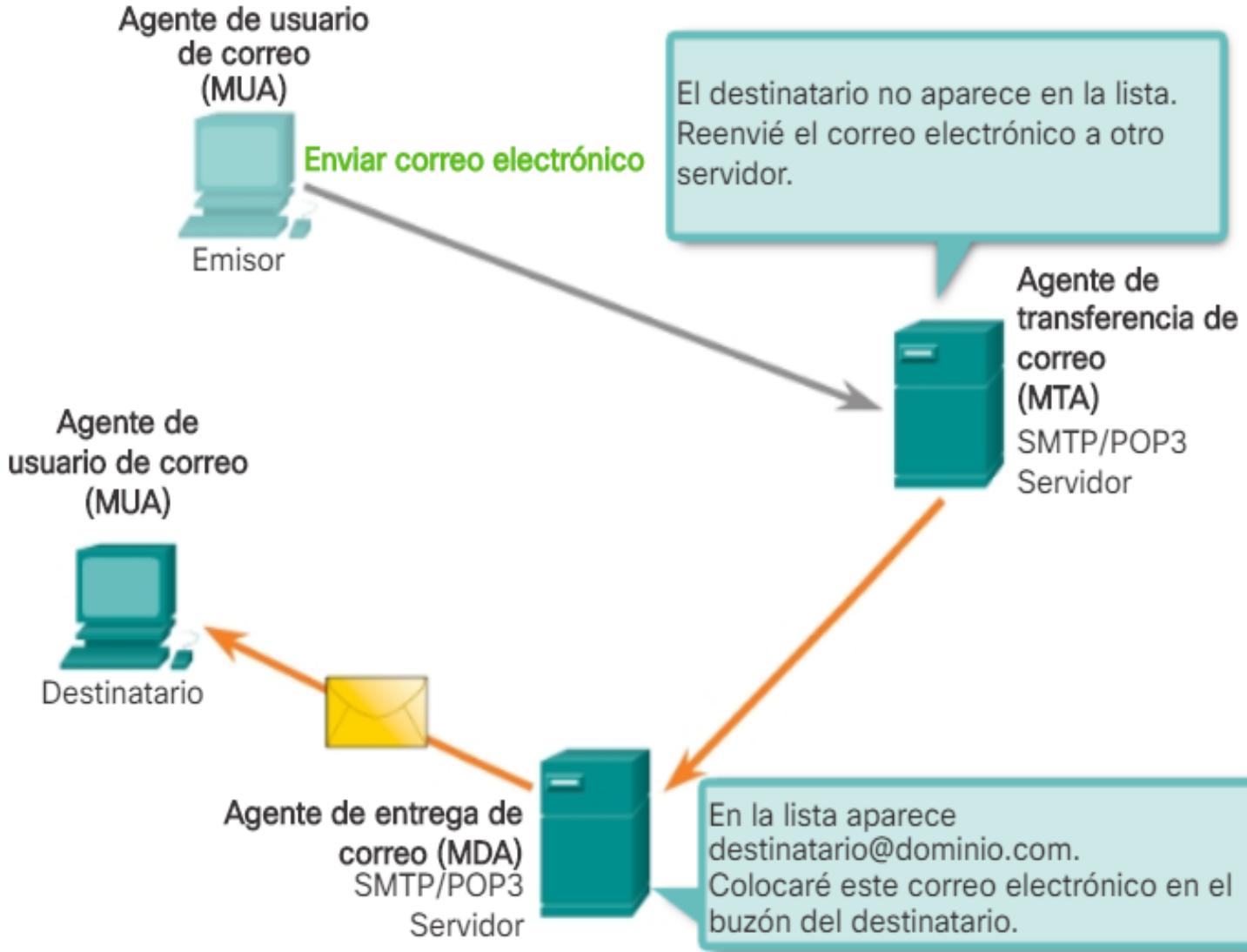
- **Redactar** un mensaje
- **Transferencia** desde el origen al destino sin intervención del usuario
- Generación de un **informe** de la transmisión del mensaje
- **Visualización** de los correos recibidos
- **Gestión** de los correos: lectura, borrado, almacenaje...

- Los **clientes de correo electrónico** se **comunican** con servidores de correo para **enviar** y **recibir** mensajes de correo electrónico según las configuraciones de aplicaciones.
- Los **servidores de correo** se **comunican** con otros servidores de correo para **transportar** mensajes desde un dominio a otro. El servidor que recibe el mensaje, verifica si el **dominio receptor se encuentra en su base de datos local**. De no ser así, envía una **solicitud de DNS** para determinar la dirección IP del servidor de correo electrónico para el dominio de destino. El correo electrónico se **reenvía** al servidor correspondiente.

El correo electrónico admite **tres protocolos diferentes** para su funcionamiento:

- el protocolo simple de transferencia de correo (**SMTP**): **envía** correo de un cliente a un servidor y cuando se envía correo de un servidor a otro
- el protocolo de oficina de correos (**POP**) para **recuperar** correo electrónico
- el protocolo de acceso a mensajes de Internet (**IMAP**), también para **recuperar** el correo electrónico, sin borrarlos del servidor. Lo que vemos es nuestro cliente es un espejo de lo que hay en el servidor.





El proceso de agente de entrega de correo rige la entrega de correo electrónico entre los servidores y los clientes.

- Cuando un cliente **envía** correo electrónico, el proceso **SMTP del cliente se conecta a un proceso SMTP del servidor** en el puerto bien conocido **25**. Una vez que el servidor recibe el mensaje, lo ubica en una cuenta local (si el destinatario es local) o lo reenvía mediante el mismo proceso de conexión SMTP a otro servidor de correo para su entrega.
- El **servidor** comienza el servicio POP **escuchando** en el puerto **110** las solicitudes de conexión del cliente.
- **MTA** (Agente Transferencia Correo), **MDA** (Agente Entrega Correo), **MUA** (Agente Usuario Correo)

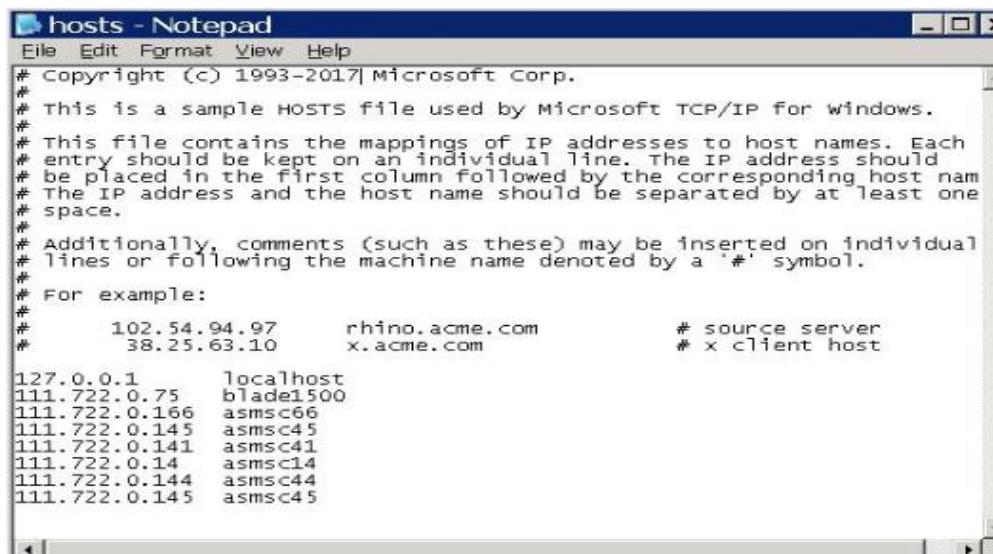
## • Servicio de nombres de dominios (DNS)

Los **dispositivos** se **etiquetan con direcciones IP numéricas** para enviar y recibir datos a través de las redes. La mayoría de las personas no puede recordar estas direcciones numéricas y **preferimos utilizar nombres** porque son más fáciles de recordar .

Los nombres de dominio se crearon para **convertir las direcciones numéricas en un nombre sencillo y reconocible**, mucho más fáciles de recordar.

Inicialmente la asociación de nombres con su respectiva dirección IP se realizaba de forma local a través del fichero:

- **/etc/hosts** (Linux)
- **\windows\system32\driver\etc\hosts** (Windows)



The image shows two screenshots of the hosts file. The left screenshot is from Microsoft Notepad on Windows, showing the sample hosts file content. The right screenshot is from a Mac OS X window, showing a similar hosts file with entries for localhost, broadcasthost, and other local addresses.

```
# Copyright (c) 1993-2017 Microsoft Corp.  
#  
# This is a sample HOSTS file used by Microsoft TCP/IP for windows.  
#  
# This file contains the mappings of IP addresses to host names. Each  
# entry should be kept on an individual line. The IP address should  
# be placed in the first column followed by the corresponding host name.  
# The IP address and the host name should be separated by at least one  
# space.  
#  
# Additionally, comments (such as these) may be inserted on individual  
# lines or following the machine name denoted by a '#' symbol.  
#  
# For example:  
#      102.54.94.97    rhino.acme.com      # source server  
#              38.25.63.10    x.acme.com        # client host  
  
127.0.0.1      localhost  
111.722.0.75    blade1500  
111.722.0.166   asmsc66  
111.722.0.145   asmsc45  
111.722.0.141   asmsc41  
111.722.0.14    asmsc14  
111.722.0.144   asmsc44  
111.722.0.145   asmsc45  
  
##  
# Host Database  
#  
# localhost is used to configure the loopback interface  
# when the system is booting. Do not change this entry.  
##  
127.0.0.1      localhost  
255.255.255.255 broadcasthost  
::1            localhost  
fe80::1%lo0    localhost  
192.168.1.xx   tickets.myvenue.org
```

Presenta varios **problemas**.

- todos los equipos de la red están obligados a conocer **cualquier cambio para actualizar sus ficheros apropiadamente**
- la inserción de un nuevo elemento en la red, debe añadirse en los **ficheros locales de cada equipo** los datos referentes a su nombre y dirección IP
- **poca escalabilidad y manejabilidad** de cualquier red local, más aún de Internet
- mantenimiento tan **descentralizado** y dependiente de ficheros locales conlleva un alto riesgo de **falta de sincronización y descoordinación** de la información que manejan

Cuando las redes eran pequeñas, resultaba fácil mantener la asignación entre los nombres de dominios y las direcciones que representaban. A medida que el tamaño de las redes y la cantidad de dispositivos aumentaron, este sistema manual se volvió **inviable**.

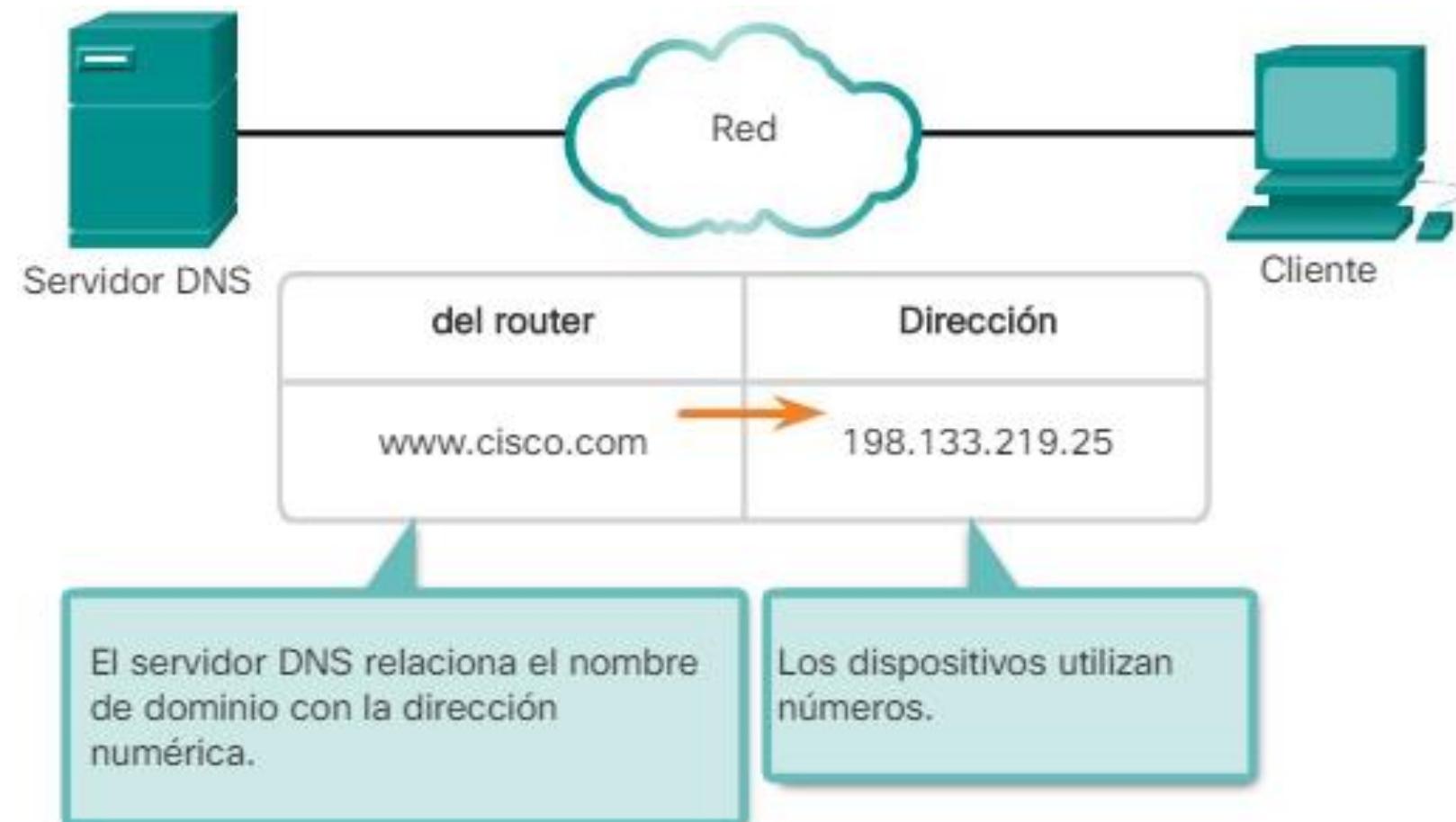
Como **ventaja** podemos decir que tenemos todos los hosts controlados y podemos hacer informes, reservas de equipos especiales, control de seguridad etc.

Para **solucionar estos problemas** se ideó el sistema de resolución de nombres (DNS) basado en dominios, en el que se **dispone de uno o más servidores encargados de resolver los nombres** de los equipos **pertenecientes a su ámbito** con sus direcciones numéricas, consiguiendo:

- **centralización** necesaria para la correcta **sincronización** de los equipos
- **sistema jerárquico** que permite una administración focalizada y descentralizada
- un mecanismo de resolución **eficiente**

#### Mostrar Recurso 10.2.2.1

Si la organización decide **cambiar** la dirección numérica es transparente para el usuario, porque el **nombre de dominio se mantiene**. Simplemente se une la nueva dirección al nombre de dominio existente y se mantiene la conectividad.



DNS utiliza un **sistema jerárquico** para crear una base de datos que proporcione la resolución de nombres. La jerarquía es similar a un árbol **invertido con la raíz en la parte superior y las ramas por debajo**. DNS utiliza nombres de domino para formar la jerarquía.

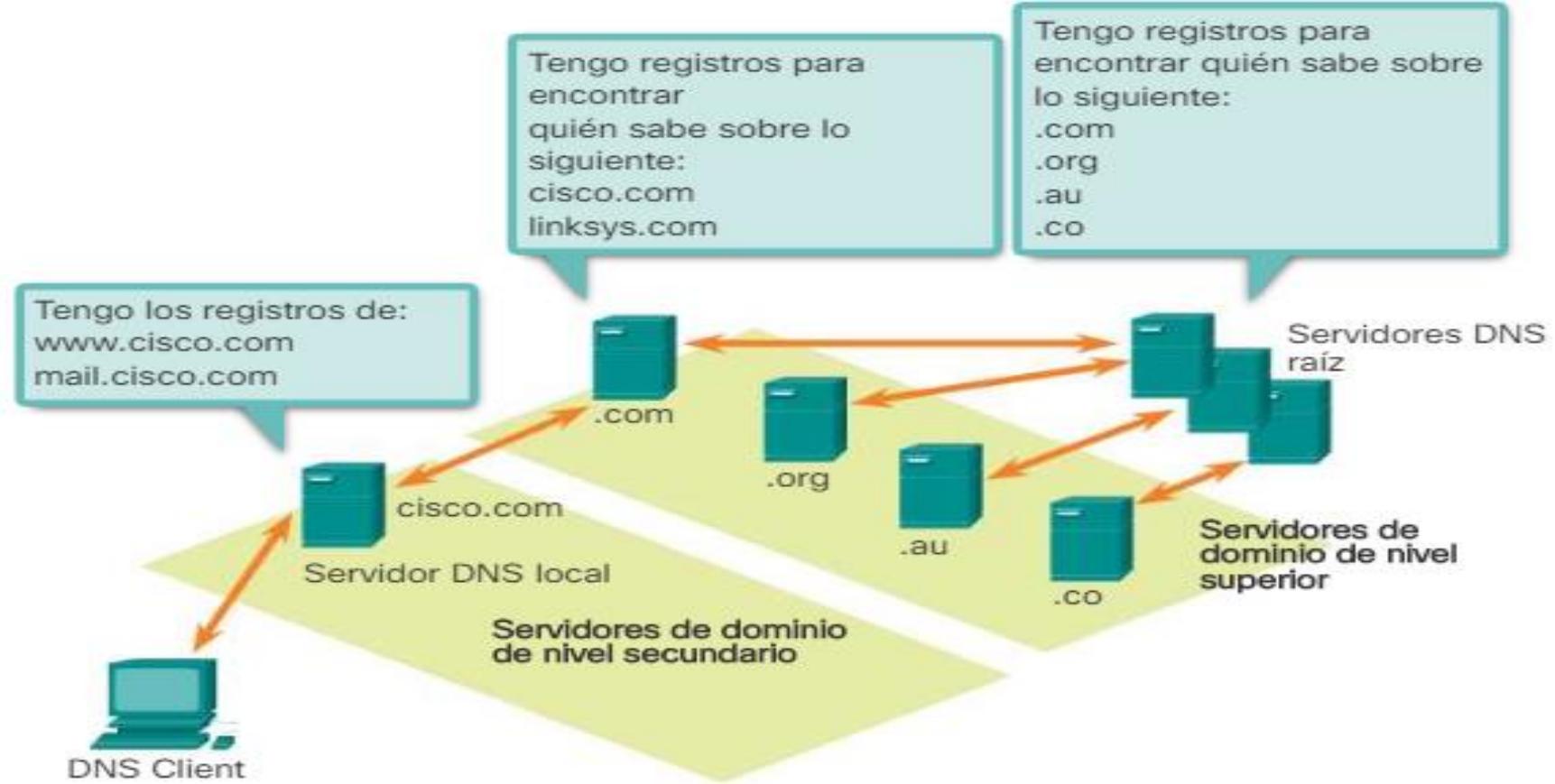
La estructura se divide en **zonas pequeñas y manejables**.

Cada **servidor DNS** mantiene un archivo de base de datos específico:

- sólo es **responsable de administrar las asignaciones de nombre a IP para esa pequeña porción** de toda la estructura DNS
- si un servidor DNS recibe una solicitud para una traducción de nombre que **no se encuentra** dentro de esa zona DNS, el servidor DNS **reenvía la solicitud a otro servidor DNS dentro de la zona adecuada para su traducción**

### Divisiones:

- Los diferentes dominios de **primer nivel** representan el tipo de organización o el país origen
- Después se encuentran los nombres de los dominios de **segundo nivel** > organizaciones
- Debajo de estos hay otros **dominios de nivel inferior** > recursos de cada organización



Cada nombre de dominio es una ruta hacia este árbol invertido que comienza de la raíz.

*Ejemplo: el servidor DNS raíz no sabe exactamente dónde se encuentra el registro del servidor de correo electrónico, **mail.cisco.com**, pero conserva un registro del **dominio .com** dentro del dominio de nivel superior. Los servidores dentro del dominio **.com** no tengan un registro de **mail.cisco.com**, pero sí tienen un registro del **dominio cisco.com**, y los servidores dentro del dominio **cisco.com** tienen un **registro para mail.cisco.com***

El servidor DNS almacena **diferentes tipos de registros (bbdd)**: recursos para **resolver nombres**. Se denomina **Zona** a la **configuración de un dominio** dentro del DNS y es un conjunto de entradas llamadas Resource Record o **RR**:

- **A**: una dirección de **dispositivo final**. Es el más utilizado y permite asociar un nombre www.mec.es con una dirección IP 193.147.0.29
- **NS (Name Server)**: **servidor** de nombre autoritativo. Indica los **servidores de DNS autorizados** (principales y secundarios) para el dominio, funciona como **delegación** de DNS de dominio (host). Permite así que **otros servidores vean los nombres de tu dominio**.
- **CNAME**: también conocido como Registro **Alias**, permite al usuario especificar el alias de un nombre de dominio, y por tanto, éste a la IP a la que está asociado el host.

*Ejemplo: **www.dominio1.com CNAME dominio1.com** que redirige a la IP del servidor donde está alojado*

- **MX**: registro de intercambio de **correos**, asigna un nombre de dominio a una lista de servidores de intercambio de correo para ese dominio específico, donde los mails deberían ser entregados.

Ejemplo: **tudominio.com** - MX - 10 **mail.tudominio.com**

donde 10 es la **prioridad**, mail.tudominio.com el **nombre** del servidor de correo.

Si tienes varios servidores de correo, puedes configurar varios registros MX con diferentes prioridades

- **SOA: Inicio** de autoridad. Fija los **parámetros de la zona**.

- **Serial**: número de serie (incremental: YYMMDDHH o timestamp de Unix)
- **Refresh**: cuándo se ha de refrescar la zona
- **Retry**: cuándo se ha de reintentar el refresh si falla
- **Expire**: a partir de cuándo se determina que una zona ya no es válida

Si desglosas el registro SOA de la [imagen de ejemplo](#) obtendrás lo siguiente:

<dominio> : esteesmidominio.com

<dns>: dns1.nominalia.com

<email>: root.dns1.nominalia.com (el @ se traduce como un punto, la dirección sería [root@dns1.nominalia.com](mailto:root@dns1.nominalia.com))

<serial>: 1440076612, timestamp de Unix. Cuenta los segundos transcurridos desde el 1 de Enero de 1970.

<refresh>: 86400 segundos

<retry>: 7200 segundos

<expire>: 2592000 segundos, expira después de un mes

<minimum>: 300, un TTL mínimo de 5 minutos

Nombre	TTL	Tipo	Valor
este es mi dominio.com.	900	A	81.88.62.2
Tipo/Valor predeterminado			
www.este es mi dominio.com	900	CNAME	este es mi dominio.com
Tipo/Valor predeterminado			

Proceso de consulta de un cliente a un servidor:

- Un **cliente** realiza una **consulta** al **servidor DNS** por un nombre.
- El servidor:
  - observa **sus propios registros** para resolver el nombre.
  - si no puede resolver con sus registros **contacta a otros servidores** para hacerlo.

La solicitud puede pasar a lo largo de **cierta cantidad de servidores**, lo cual puede tomar más **tiempo** y consumir **ancho de banda**. Una vez que se encuentra una coincidencia y se la devuelve al servidor solicitante original, este **almacena** temporalmente en la **memoria caché** el registro. Si un cliente solicita ese mismo nombre, utiliza el valor almacenado en el caché.

Esto **reduce el tráfico en la red** de consultas DNS, los **tiempos de espera** y las **cargas de trabajo** de los servidores más altos de la jerarquía.

### Adaptador de LAN inalámbrica Wi-Fi:

Sufijo DNS específico para la conexión . . . : Home  
Descripción . . . . . : Intel(R) Dual Band Wireless-AC 3165  
Dirección física . . . . . : B4-6B-FC-3A-DC-39  
DHCP habilitado . . . . . : sí  
Configuración automática habilitada . . . . : sí  
Vínculo: dirección IPv6 local . . . . : fe80::fc8f:c6b4:df91:f203%19(Preferido)  
Dirección IPv4 . . . . . : 192.168.1.132(Preferido)  
Máscara de subred . . . . . : 255.255.255.0  
Concesión obtenida . . . . . : miércoles, 23 de enero de 2019 22:35:38  
La concesión expira . . . . . : domingo, 27 de enero de 2019 8:47:21  
Puerta de enlace predeterminada . . . . . : fe80::1%19  
  192.168.1.1  
Servidor DHCP . . . . . : 192.168.1.1  
IAID DHCPv6 . . . . . : 297036796  
DUID de cliente DHCPv6 . . . . . : 00-01-00-01-23-13-46-69-00-80-8E-8A-93-43  
Servidores DNS . . . . . : fe80::1%19  
  192.168.1.1 [REDACTED]

### Detalles de la conexión de red

#### Detalles de la conexión de red:

Propiedad	Valor
Sufijo DNS específico p...	Home
Descripción	Intel(R) Dual Band Wireless-AC 3165
Dirección física	B4-6B-FC-3A-DC-39
Habilitado para DHCP	Sí
Dirección IPv4	192.168.1.132
Máscara de subred IPv4	255.255.255.0
Concesión obtenida	miércoles, 23 de enero de 2019 22:35:38
La concesión expira	domingo, 27 de enero de 2019 8:47:21
Puerta de enlace predet...	192.168.1.1
Servidor DHCP IPv4	192.168.1.1
Servidor DNS IPv4	192.168.1.1
Servidor WINS IPv4	
Habilitado para NetBios ...	Sí
Vínculo: dirección IPv6 l...	fe80::fc8f:c6b4:df91:f203%19
Puerta de enlace predet...	fe80::1%19
Servidor DNS IPv6	fe80::1%19



Si quieres obtener más información, puedes ver más información sobre el servicio DNS.

[http://es.wikipedia.org/wiki/Domain\\_Name\\_System](http://es.wikipedia.org/wiki/Domain_Name_System)

El comando **ipconfig /displaydns** muestra todas las entradas DNS en caché en un sistema de computación Windows.

```
papassegedu.jccm.es
-----
Nombre de registro . . . : papassegedu.jccm.es
Tipo de registro . . . : 1
Período de vida . . . : 16829
Longitud de datos . . . : 4
Sección . . . . . : respuesta
Un registro (host). . . : 89.107.244.26
```

Al configurar un **dispositivo de red** proporcionamos una o más **direcciones del servidor DNS** que el **cliente DNS** puede utilizar para la resolución de nombres.

En general, el **proveedor** de servicios de Internet (**ISP**) suministra las direcciones para utilizar con los servidores DNS.

Los sistemas operativos de los PC cuentan con una **utilidad** llamada “nslookup” que permite que el **usuario consulte los servidores de nombres de forma manual para resolver un nombre de host determinado**.

Puede utilizarse para **solucionar los problemas de resolución de nombres y verificar el estado actual** de los servidores de nombres. **Muestra el servidor DNS predeterminado** configurado para tu host. Se pueden **hacer consultas sobre un host determinado**.

```
C:\Users\Alfonso>nslookup  
Servidor predeterminado: UnKnown  
Address: 192.168.0.1  
  
> www.riberadeltajo.es  
Servidor: UnKnown  
Address: 192.168.0.1  
  
Respuesta no autoritativa:  
Nombre: www.riberadeltajo.es  
Address: 217.160.230.163  
  
> www.cisco.com  
Servidor: UnKnown  
Address: 192.168.0.1  
  
Respuesta no autoritativa:  
Nombre: e2867.dsca.akamaiedge.net  
Addresses: 2a02:26f0:15:1:8100::b33  
           2a02:26f0:15:1:9c00::b33  
           23.37.160.19  
Aliases: www.cisco.com  
         www.cisco.com.akadns.net  
         wwwds.cisco.com.edgekey.net  
         wwwds.cisco.com.edgekey.net.globalredir.akadns.net  
  
> www.talaveradelareina.es  
Servidor: UnKnown  
Address: 192.168.0.1  
  
*** UnKnown no encuentra www.talaveradelareina.es: Non-existent domain
```

- El **servidor DNS** es 192.168.0.1
  - El **nombre de un host** o de un dominio se puede introducir en la petición de entrada de nslookup. Se hace una **consulta** para www.cisco.com. El **servidor** de nombre que **responde** proporciona la dirección 23.37.160.19
- exit** para salir de la utilidad nslookup

La utilidad nslookup tiene **muchas opciones disponibles para realizar una prueba y una verificación exhaustivas del proceso DNS.**

- **Protocolo de Configuración Dinámica de Host - DHCP**

El servicio DHCP permite a los dispositivos de una red **obtener direcciones IP y más información** de un **servidor DHCP**.

Este servicio **automatiza** la asignación de direcciones IP, máscaras de subred, gateway y otros **parámetros** de redes IP.

Esto se denomina “**direcccionamiento dinámico**”. La alternativa al direccionamiento dinámico es el direccionamiento **estático**.

Al utilizar el direccionamiento estático, el **administrador de red introduce manualmente la información de la dirección IP en los hosts de red**.

Cuando un host se **conecta** a la red, realiza el **contacto con el servidor** de DHCP y se **solicita** una dirección. El servidor de DHCP **elige** una dirección de un rango de direcciones configurado llamado “**pool**” y le asigna (**concede**) al host por un **período establecido**.

En redes locales más **grandes**, o donde los **usuarios cambian con frecuencia**, se prefiere asignar direcciones con DHCP. Es **más eficaz**, que en lugar que el administrador de red tenga que estar asignando direcciones IP para cada estación de trabajo.

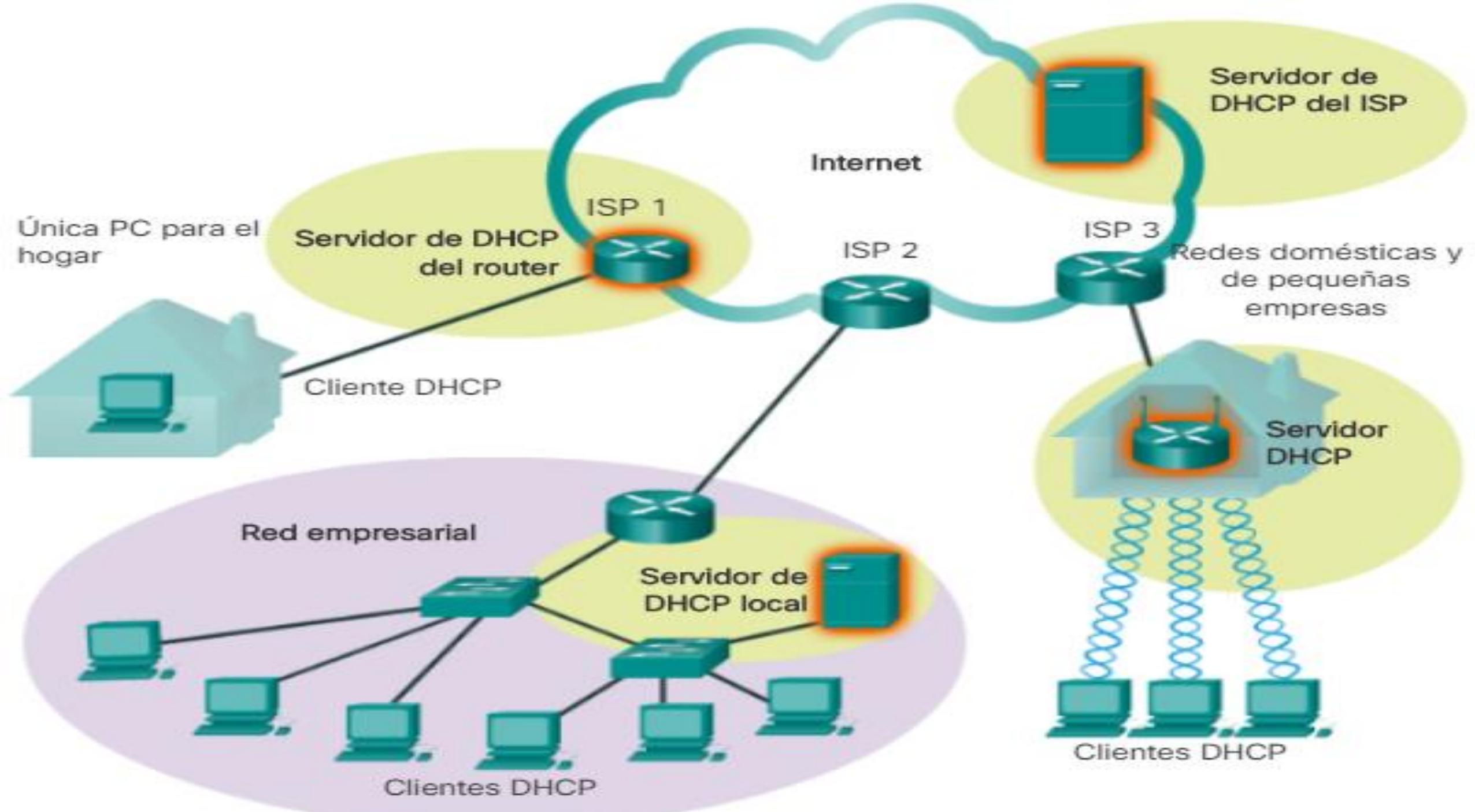
Las direcciones por DHCP **no se asignan de forma permanente** a los hosts, sino que solo se conceden por un cierto período. Si el host se apaga o se desconecta de la red, la dirección regresa al pool para volver a utilizarse.

En la mayoría de las **redes medianas a grandes**, el servidor de DHCP suele ser un servidor local dedicado con base en un PC. En las **redes domésticas**, el servidor de DHCP suele estar ubicado en el router local que conecta la red doméstica al ISP. Los hosts locales reciben la información de la dirección IP directamente del router local. El router local recibe una dirección IP del servidor de DHCP en el ISP.

DHCP puede representar un **riesgo a la seguridad** porque cualquier dispositivo conectado a la red puede recibir una dirección.

Muchas redes **combinan** tanto el direccionamiento estático como dinámico:

- **DHCP** se utiliza para hosts de uso general, como los dispositivos para usuarios finales.
- **direcciónamiento estático** se utiliza para dispositivos de red, como gateways, switches, o máquinas que requieran un direcciónamiento especial, como servidores e impresoras.

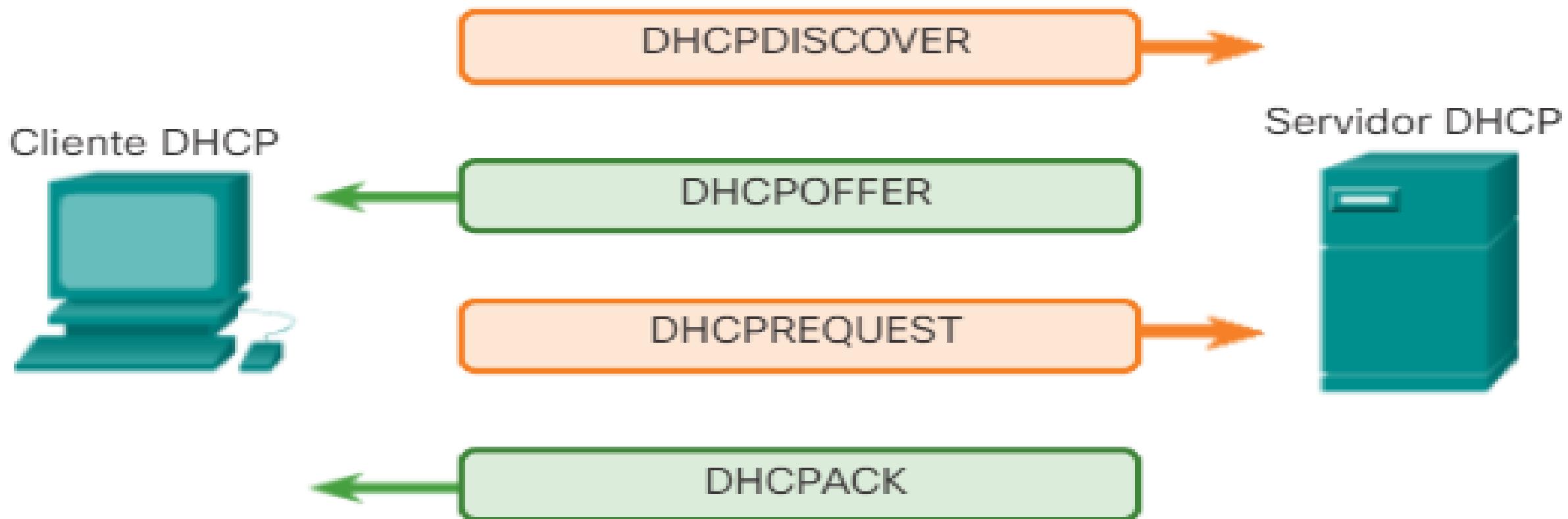


## Funcionamiento de DHCP

El servidor de DHCP mantiene un **pool** de las direcciones IP y **alquila** una dirección a cualquier cliente habilitado por DHCP cuando el cliente está activado. Las direcciones IP son dinámicas y cuando **están en desuso regresan automáticamente al pool** para que se vuelvan a asignar.

- Cuando un dispositivo configurado con DHCP se inicia o se **conecta** a la red, el cliente **transmite** un mensaje de descubrimiento de DHCP (**DHCPDISCOVER**) para **identificar** cualquier **servidor de DHCP disponible en la red**.
- Un **servidor** de DHCP **responde** con un mensaje de oferta de DHCP (**DHCPOFFER**), que ofrece una concesión al cliente. El mensaje de oferta **contiene**: dirección IP, máscara de subred que se debe asignar, dirección IP del servidor DNS, dirección IP del gateway y la duración.
- El **cliente** **envía** un mensaje de solicitud de DHCP (**DHCPREQUEST**) que identifique el servidor y la oferta de concesión que el cliente acepta.
- El **servidor** **devuelve** un mensaje de acuse de recibo de DHCP (**DHCPACK**) que le confirma al cliente de la concesión. Si la oferta ya no es válida, quizá debido a que hubo un tiempo de espera o a que otro cliente tomó la concesión, entonces el servidor seleccionado responde con un mensaje de acuse de recibo negativo de DHCP (**DCHPNACK**).

- Si se devuelve un mensaje DHCPNACK, entonces el proceso de selección debe volver a **comenzar con la transmisión de un nuevo mensaje DHCPDISCOVER**.
- Una vez que el cliente tiene la concesión, se debe **renovar** mediante otro mensaje **DHCPREQUEST** antes de que expire.
- El servidor de DHCP asegura **que todas las direcciones IP sean únicas** (no se puede asignar la misma dirección IP a dos dispositivos de red diferentes de forma simultánea).



```

#
# DHCP Server Configuration file.
#   see /usr/share/doc/dhcp*/dhcpd.conf.example
#   see dhcpd.conf(5) man page
#
option domain-name "zero.net";
option domain-name-servers 8.8.8.8;
option subnet-mask 255.255.255.0;
option routers 172.16.100.1;
default-lease-time 86400;
max-lease-time 691200;
min-lease-time 3600;
subnet 172.16.100.0 netmask 255.255.255.0 {
    range 172.16.100.2 172.16.100.99;
}_

```

**DHCP**

Servicios	<input checked="" type="radio"/> Encendido	<input type="radio"/> Apagado		
Pool Name	DHCP_P1			
Gateway por Defecto	201.10.220.90			
Servidor DNS	201.10.220.90			
Inicio de la Dirección IP:	201	10	248	0
Subnet Mask:	255	255	252	0
<pre>R1(config)# ip dhcp excluded-address 192.168.10.1 192.168.10.9 R1(config)# ip dhcp excluded-address 192.168.10.254 R1(config)# ip dhcp pool LAN-POOL-1 R1(dhcp-config)# network 192.168.10.0 255.255.255.0 R1(dhcp-config)# default-router 192.168.10.1 R1(dhcp-config)# dns-server 192.168.11.5 R1(dhcp-config)# domain-name example.com R1(dhcp-config)# end R1#</pre>				

*Si quieres obtener más información, puedes ver más información sobre el servicio DHCP.*

[http://es.wikipedia.org/wiki/Dynamic\\_Host\\_Configuration\\_Protocol](http://es.wikipedia.org/wiki/Dynamic_Host_Configuration_Protocol)

- **Servicio de acceso remoto.**

Permiten acceder de forma **remota** a un equipo a través de la **red**.

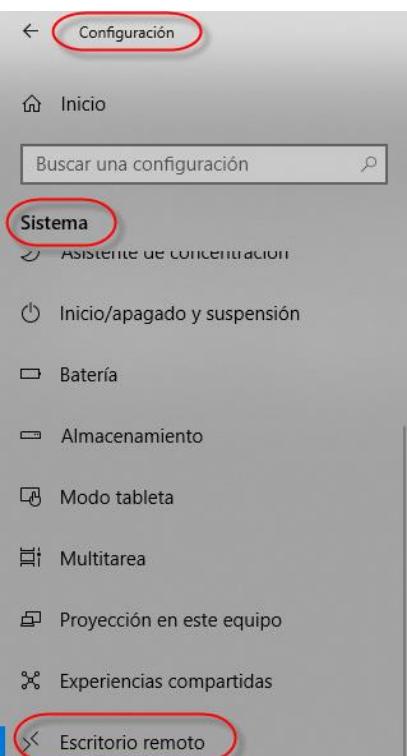
Dos **categorías**:

- Acceso remoto en modo **terminal**. Para acceder a un equipo Linux en modo terminal es posible utilizar los servicios **Telnet** (Telecommunication NETwork) y **SSH** (Secure SHell). SSH es el más utilizado ya que garantiza la **seguridad** de las comunicaciones, Telnet no se utiliza por ser inseguro.
- Acceso remoto en modo **gráfico**. Se puede utilizar el servicio **VNC**, el servicio de **Escritorio remoto** (Terminal Server) en sistemas Windows, o **TeamViewer**.



# ¿Qué servicio permite conectarse a un servidor de forma remota por terminal?

- Telnet
- VNC
- Terminal Server
- SSH



## Escritorio remoto

### Escritorio remoto

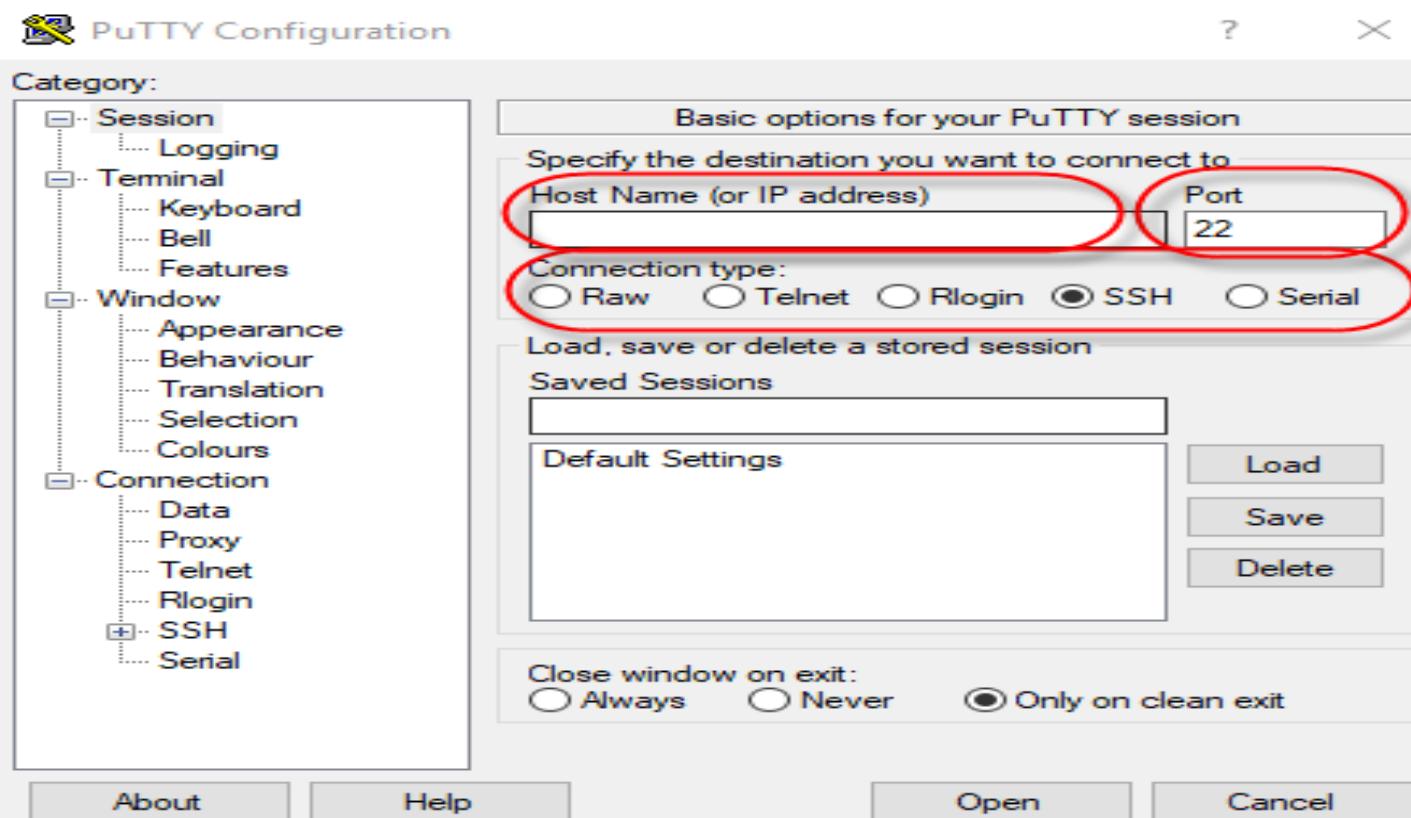
Escritorio remoto te permite conectarte a y controlar este equipo desde un dispositivo remoto mediante la aplicación de un cliente de Escritorio remoto (disponible para iOS, Android, Mac y Windows). Podrás trabajar desde otro dispositivo, como si estuvieras trabajando directamente en este equipo.

#### Habilitar Escritorio remoto

Desactivado

### Cuentas de usuario

Seleccione los usuarios que pueden tener acceso remoto a este equipo



- **Protocolo de transferencia de archivos (FTP).**

Protocolo de capa de aplicación que se utiliza para permitir **las transferencias de datos** entre un cliente y un servidor.

Un **cliente** FTP es una aplicación que se ejecuta en un PC y que se utiliza para **insertar y extraer datos** en un **servidor**.

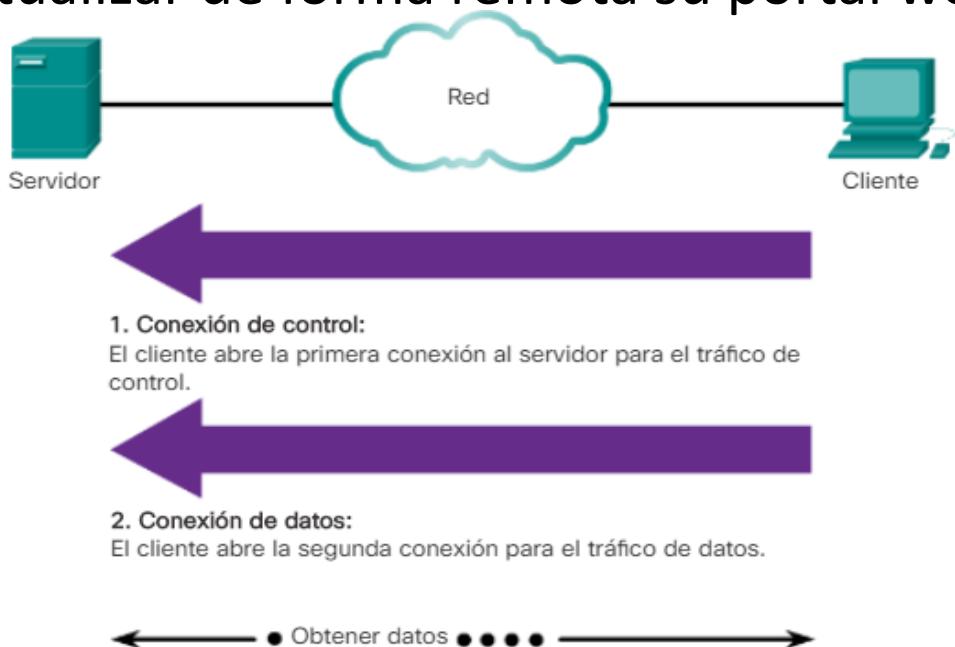
Un **servidor** FTP es una aplicación que se ejecuta en un PC y que se utiliza para albergar datos. El servidor ejecuta un servicio o **demonio** FTP (FTPD).

FTP requiere **dos conexiones** entre el cliente/servidor, una para **comandos** y respuestas (control) **puerto20**, y la otra para la **transferencia** de archivos propiamente dicha, **puerto21**

- El cliente establece la **primera** conexión al servidor para el **tráfico de control**, que está constituido por **comandos del cliente y respuestas del servidor**.
- El cliente establece la **segunda** conexión al servidor para la **transferencia** de datos propiamente dicha. La transferencia de datos se puede producir en **ambas direcciones**. El cliente puede **descargar** datos del servidor o **subir** datos a él

Hay dos tipos fundamentales de **acceso** a través de FTP:

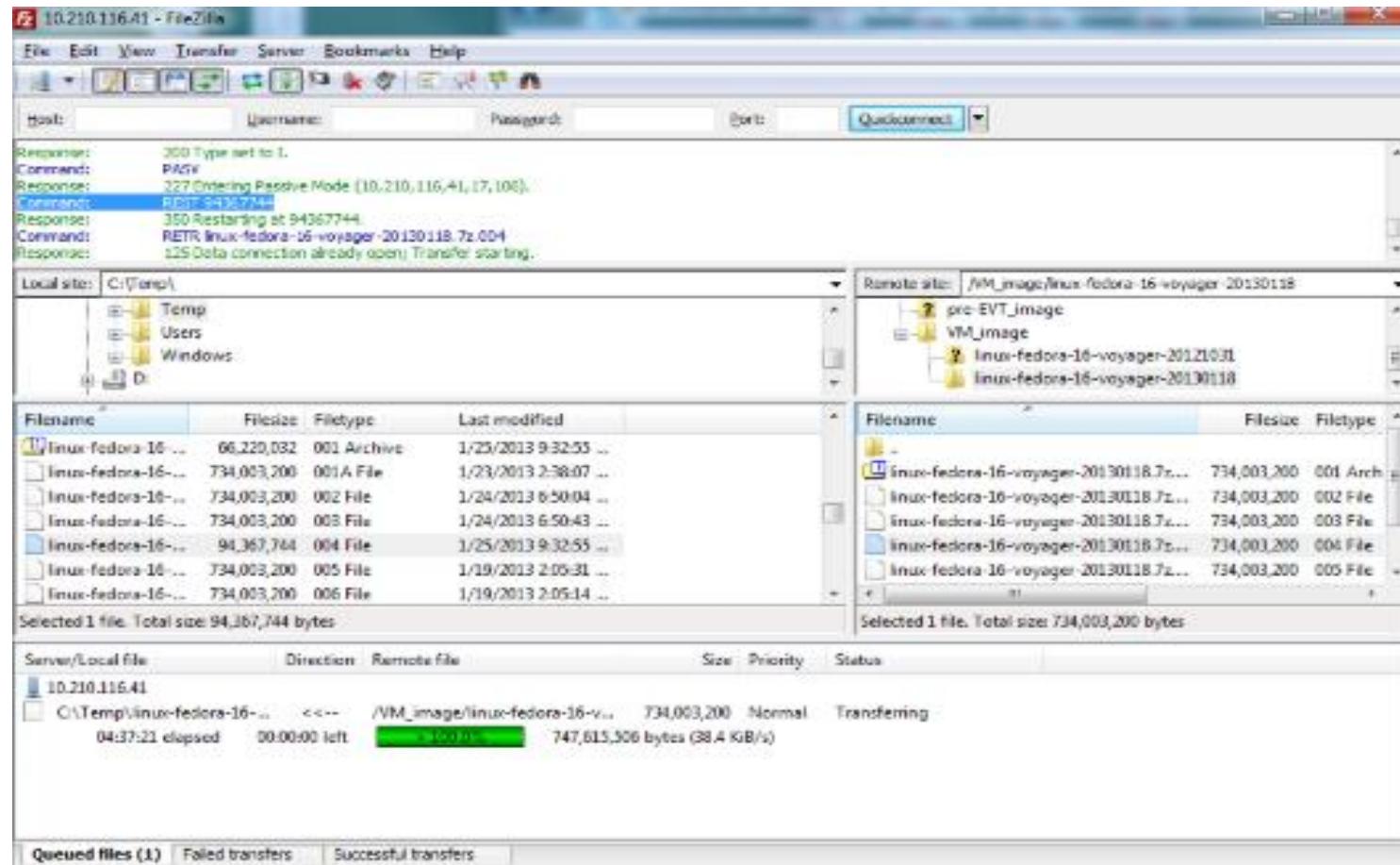
- **Anónimo:** la comunicación se realiza **sin ningún tipo de identificación** y, por lo tanto el usuario tendrá muy **pocos privilegios** en el servidor. El usuario estará confinado en un **directorio público** donde puede **descargar** los archivos allí ubicados pero sin posibilidad de escribir o modificar ningún fichero.
- **Autorizado:** el usuario establece la comunicación con una **cuenta de usuario**. Tras identificarse, el usuario cuenta con su **directorio predeterminado** desde donde puede **descargar ficheros** y, si la política del sistema lo permite, también **escribir**. Esta opción es ampliamente utilizada para que los usuarios puedan acceder a sus ficheros o para poder actualizar de forma remota su portal web.



Nombre	Tamaño	Fecha de modificación
README.TXT	4.2 kB	7/5/15 2:00:00
TIMESTAMP	35 B	25/1/19 11:00:00
development/		25/1/19 11:00:00
dir.sizes	5.1 kB	25/1/19 11:00:00
doc/		12/11/17 1:00:00
ports/		12/11/17 1:00:00
releases/		25/1/19 11:00:00
snapshots/		9/11/18 23:47:00

## Clientes que permiten conectarse a un servidor FTP:

- **Gráficos:** filezilla, cuteftp, vsftpd
- **Terminal:** la forma más simple de utilizar un servidor FTP es estableciendo una conexión por **línea de comandos**. Ejecutar programa servidor FTP. Utilizando los comandos FTP, sin importar el sistema operativo que utilices, puedes trabajar en el servidor FTP.



### Actividad 3.2.2.4 Protocolos y Capas

Actividad. Rellena los espacios en blanco

Instalar Filezilla Server-Client y conectar con algún PC del aula. Probar los comandos FTP.

### 10.2.3.3 Exploring FTP