SISTEMAS EN RED. INTRODUCCIÓN

CONCEPTOS SOBRE REDES

DEFINICIÓN DE RED

Una red de ordenadores es un sistema de interconexión entre equipos que permite compartir recursos e información. Para ello, es necesario contar, además de con los ordenadores correspondientes, con las tarjetas de red, los cables de conexión los dispositivos de comunicación y el software conveniente. Entre las ventajas de una red encontramos:

- Compartir programas y archivos
- Compartir recursos de la red, como impresoras, MODEM, fax...
- Compartir grandes cantidades de información, bases de datos, etc.
- Reduce la duplicidad de trabajos
- Posibilidad de trabajo en grupo
- Gestión de recursos centralizada
- Seguridad
- Interconectividad
- Mejoras en la organización de la empresa

TIPOS DE REDES

Por localización geográfica

La localización geográfica de la red es un factor a tener en cuenta a la hora de diseñarla y montarla. No es lo mismo montar una red en un aula de informática que interconectar 2 sucursales de una empresa en diferentes países.

- **Subred o segmento de red:**

Un segmento de red está formado por un conjunto de estaciones que comparten el mismo medio de transmisión. El segmento está limitado en espacio al departamento de un empresa, aula de informática, etc. Se considera como la red de comunicación más pequeña y todas las redes de mayor tamaño están compuestas por la unión de varios segmentos de red

- **Redes de área local (LAN – Local Area Network).**

Abarcan un mismo edificio o empresa, con una extensión máxima de una decena de kilómetros.

- **Redes metropolitanas (MAN – Metropolitan Area Network).**

Puede abarcar una ciudad completa y está sujeta a regulaciones locales. Puede constar de recursos públicos y privados, como el sistema de telefonía local, microondas locales o cables de fibra óptica. Una empresa local construye y mantiene la red, y la pone a disposición del público. Puede conectar sus redes a la MAN y utilizarla para transferir información entre redes de otras ubicaciones de la empresa dentro del área metropolitana.

- **Redes extensas (WAN – World Area Network)**

Normalmente están compuestas por varias LAN interconectadas entre sí, ubicadas en distintas partes de un país o del mundo.

COMPONENTES DE UNA RED

COMPONENTES LÓGICOS

• EL SISTEMA OPERATIVO

Para permitir trabajar a los clientes con todos los recursos compartidos en la red, es necesario que el sistema operativo sea capaz de realizar acciones como la transmisión de los datos a través de la red , controlar la seguridad de la conexión, gestionar el acceso a los recursos por parte de todos los usuarios, etc.

Los principales sistemas operativos en red son: Windows Server, Unix, Linux….

• SERVIDOR

Es un ordenador/es que permite compartir sus periféricos con otros ordenadores. Entre otros podemos encontrar:

- **Servidor de archivos:** Mantiene archivos en subdirectorios privados o compartidos para los usuarios de la red
- **Servidor de impresión**: Tiene conectada una o más impresoras que comparte con el resto de los usuarios
- **Servidor de comunicaciones:** Permite enlazar diferentes redes locales o una red local con grandes ordenadores o miniordenadores
- **Servidor de correo electrónico:** Proporciona servicios de correo electrónico para la red
- **Servidor web**: Proporciona un lugar para guardar y administrar los documentos HTML que pueden ser accesibles por los usuarios de la red a través de los navegadores
- **Servidor FTP**: Se utiliza para guardar los archivos que pueden ser descargados por los usuarios de la red
- **Servidor proxy:** Se utiliza para monitorizar el acceso entre las redes. Cambia la dirección IP de los paquetes de los usuarios para ocultar los datos de la red interna a Internet y, cuando recibe contestación externa la devuelve al usuario que la ha solicitado. Su uso reduce la amenaza de piratas que visualicen el tráfico de la red para conseguir información sobre los ordenadores de la red interna.

Los servidores de una red pueden ser dedicados, cuando utilizan todos sus recursos para dar servicio a los clientes, sin ejecutar ninguna otra aplicación, y no dedicados, cuando ejecutan aplicaciones distintas a los servicios que ofrecen a la red.

ESTACIONES DE TRABAJO.

Son puestos conectados a la red que utilizan los usuarios para acceder a los recursos de los servidores.

COMPONENTES FÍSICOS

Para que la red pueda funcionar correctamente, es necesario conectar físicamente los ordenadores. Los componentes que interconectan los equipos informáticos son los siguientes:

CABLES

Hay varios tipos de cables:

- **CABLE COAXIAL.**

  Está formado por una malla de cobre entrelazado que protege al hilo conductor central de las corrientes eléctricas externas. Es económico, la velocidad es alta y la longitud puede ser mayor que el cable UTP. Utiliza conectores BNC.

- **CABLE PAR TRENZADO**

  El cable par trenzado está formado por pares de cobre, de forma que cada par está entrelazado con objeto de evitar o reducir interferencias. Las interferencias suelen subsanarse con el uso de una tela metálica que cubre a todos los grupos de pares que forman un cable o a cada par de hilos.

  Tipos de cables par trenzados:

  - UTP (Unshield Twisted Pair - Par trenzado sin apantallar). Son hilos de cobre sin apantallar, es decir, no tienen malla metálica protectora. Son los más económicos, pero son menos fiables, ya que sólo reducen interferencias con el trenzado del cable.

  - FTP (Foiled Twisted Pair - Par trenzado con pantalla global). Dispone de malla de protección pero no cubre todos los hilos de cobre.

  - STP (Shielded Twisted Pair – Par trenzado apantallado) Cada par de hilos de cobre, además de estar trenzado dispone de una malla que los recubre. Es el más fiable y el más caro.

- **CABLE DE FIBRA ÓPTICA.**

  Transporta pulsos de luz a través de pequeñas fibras de vidrio, por lo que no le afectan las corrientes externas. Consta de dos hilos de fibra de vidrio, cada uno de los cuales transmite en una sola dirección. Son más caros que los anteriores, pero su velocidad de transmisión es muy alta (hasta 200Gbps) y su longitud puede ser muy elevada. Utilizan conectores especiales ST (los más antiguos) y SC (que integra dos fibras).

DISPOSITIVOS DE INTERCONEXIÓN

DISPOSITIVOS HARDWARE DE NIVEL FÍSICO

REPETIDORES

Dispositivos que amplifican la señal digital, en interconexiones de largas distancias. Estos dispositivos restauran la señal original permitiendo que alcance el equipo receptor de la información.

CONCENTRADORES

Los concentradores o centrales de cableado son dispositivos físicos encargados de replicar la señal a todos los ordenadores conectados a él, un concentrador esta caracterizado por el número de terminales que puede conectar, este número de terminales se le suele llamar número de puertos de tal forma que cada terminal se conectará a un puerto del concentrador.

El número de puertos de un concentrador puede variar siendo los típicos de 4, 8, 16, 24 y 32 puertos del tipo RJ-45 existen varios tipos de concentradores:

DISPOSITIVOS HARDWARE DE NIVEL DE ENLACE

El uso de dispositivos de nivel físico para conectar nodos de una red es una solución sencilla y útil cuando hay pocos ordenadores y no esperamos un rendimiento elevado. Ej. Utilizando hub para conectar una red, cada paquete se propaga por todos los puertos del dispositivo, lo que reduce la velocidad de transferencia.

Por otro lado, podemos tener una red local montado en distintos edificios con diferentes estándares 802.3, 802.11, 802.5, etc. y deben estar conectadas entre sí. para ello se necesitan dispositivos de nivel de enlace

Los dispositivos de nivel de enlace trabajan con direcciones MAC (Media Access Control) o direcciones físicas. Una dirección MAC identifica de forma única a una tarjeta o dispositivo de red.

NIC. TARJETAS DE RED

Es la interfaz de comunicación entre el ordenador y el medio de transmisión (cables). Contiene un controlador que transforma los datos en paralelo, que es como los emite el ordenador, en datos en serie, que es como se transmiten por el medio de transmisión. Los datos procedentes de otro ordenador siguen el proceso inverso.

Por todo esto, la tarjeta de red cumple la función de CODEC (codificador- decodificador), convirtiendo las señales digitales en analógicas y viceversa.

Cada tarjeta de red tiene una dirección física o dirección MAC única.

Existen diferentes tipos en función de la arquitectura o cableado de red que se utilice (adaptadores de red

Ethernet, Token Ring, inalámbricas, etc.)

SWITCHES

Son dispositivos físicos que actúan a nivel de enlace de la OSI, que surgieron como mejora a los concentradores. Un switch es capaz de analizar una trama de nivel de enlace y difundir la información sólo a los puertos necesarios (no a todos como hace el hub). Hoy en día, es la opción más interesante debido a que mejora el funcionamiento de una red de área local y su coste no es muy elevado. También, se caracteriza por el número de puertos pero gracias a esa capacidad de análisis de tramas el número de puertos puede llegar a ser extremadamente altos (hasta los 2000 puertos.

Conecta redes que utilicen el mismo protocolo.

PUNTO DE ACCESO INALÁMBRICO. AP

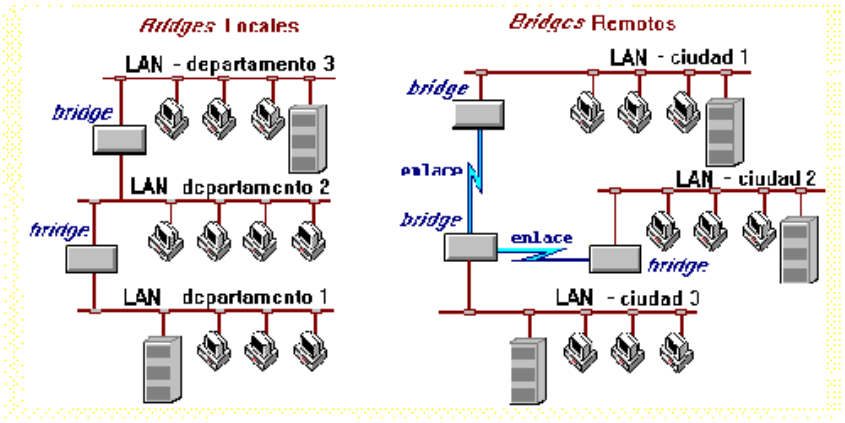
Interconecta dispositivos inalámbricos para formar una red inalámbrica. Normalmente un AP tiene una serie de puertos RJ45 que le permiten conectar con la red cableada pudiendo enviarse información desde la red inalámbrica a la cableada. Un AP es un repetidor, ya que los paquetes los almacena y los transmite a todos los puestos inalámbricos y cableados.

BRIDGES

Es el dispositivo encargado de conectar a nivel de enlace redes con topologías y protocolos diferentes

Está formado por al menos dos interfaces diferentes, una por cada tipo de red que conecta.

Este dispositivo también controla el tráfico de red de forma que no deja pasar a través de él cualquier paquete que no esté remitido a la otra red. No permiten el paso de BROADCAST.



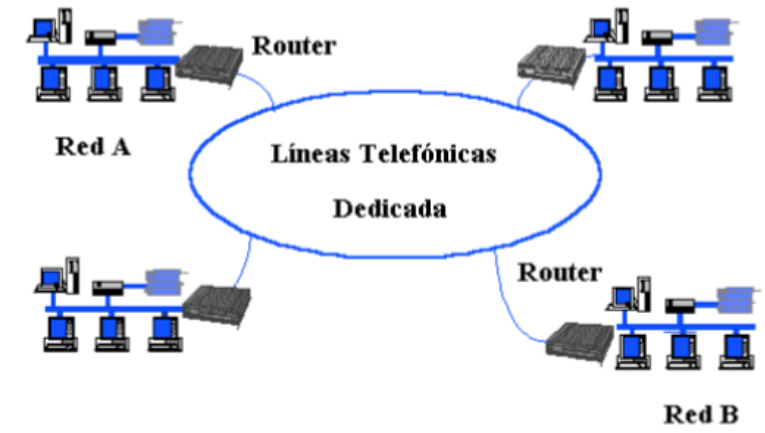
DISPOSITIVOS HARDWARE DE NIVEL DE RED

ROUTERS

También llamado servidor de comunicaciones, son dispositivos que operan a nivel de Red y que se encargan de comunicar diferentes redes de comunicaciones, estos routers llevan implementados mecanismos complejos para inspeccionar el tráfico y saber encaminar la información hacia su destino. Tienen también la capacidad de filtrado de la información, es decir, son capaces de permitir o no el acceso de determinada información a determinados destinos en base a los siguientes criterios:

- Filtrar la información con destino a una determinada dirección IP ya sea de red o de HOST.
- Filtrar la información con origen una determinada IP ya sea de red o de HOST.
- Filtrar la información con destino a un puerto determinado de una entidad de transporte.(ejemplo: no permitir el paso al puerto 80:TCP o lo que es lo mismo no permitamos a usuarios exteriores a nuestra red el paso a nuestro servidor web).
- Filtrar la información con origen un puerto determinado.
- Filtrar un determinado tipo de información.

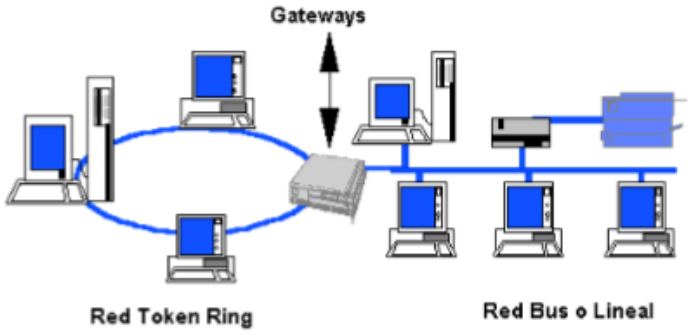
Un enrutador está programado para leer una gran cantidad de protocolos.



DISPOSITIVOS HARDWARE DE NIVEL DE APLICACIÓN

GATEWAYS

Funcionan a nivel de aplicación. Es un dispositivo ya sea hardware o software, que conecta dos tipos distintos de redes de comunicaciones Realiza conversión de protocolos de una red a otra.

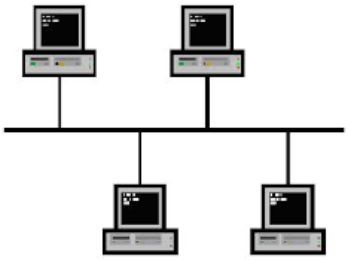


Ejemplo:Conectar una red de tipo Ethernet (IEEE 802.3) con una red de tipo inalámbrica (IEEE802.11b).

TOPOLOGÍAS

Topología en BUS

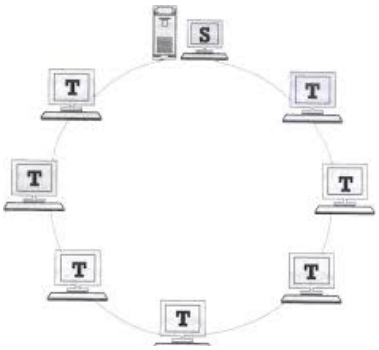
Es la topología más simple, en la que un único tendido, mediante derivaciones, da servicio a todos y cada uno de los terminales, por lo que, en caso de fallo, una parte de la red queda siempre sin servicio.



Suele emplearse para esta topología cable coaxial, y el ejemplo más típico de la misma lo constituyen las redes Ethernet en bus. La estructura puede complicarse añadiendo ramificaciones hasta llegar a formar un árbol (topología en árbol).

Topología en ANILLO

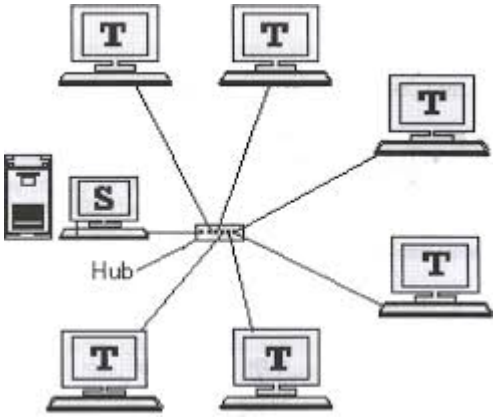
Es una variante de la topología en bus, en la que éste se cierra sobre sí mismo, por lo que, en caso de rotura, se puede acceder a las estaciones aisladas por el otro semianillo.



En la práctica, la mayoría de las topologías en anillo (lógica) acaban siendo una estrella física. Pueden emplearse cables de pares, coaxiales o fibra óptica. Esta topología encuentra su ejemplo más significativo en las redes Token Ring.

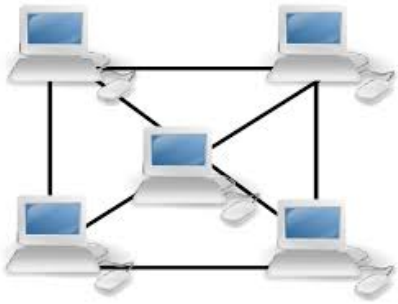
Topología en ESTRELLA

En esta topología, un elemento central (HUB) sirve de puente entre todos los terminales de la LAN, proporcionando la conmutación entre ellos. Aisla unos elementos del fallo de otros, pero presenta como punto crítico el nodo central, que, en caso de fallo, deja la red sin servicio. El coste del cableado es elevado al requerir conexiones punto a punto para todos los elementos, aunque éste se minimiza empleando cable par trenzado.



Topología de MALLA

Es la topología que ofrece un mayor nivel de seguridad. Los nodos de la red se unen entre sí formando una estructura en la que al menos existen dos rutas posibles en cada nodo; así, si hay un fallo en una de ellas la información puede hacerse circular por la otra. Es una topología adecuada para cubrir, por ejemplo, un país completo. En particular, es la red que utilizaba Telefónica para su red Iberpac.



PROTOCOLOS Y SERVICIOS DE RED

Un protocolo es un conjunto de reglas y convenciones comunes entre participantes en la comunicación. Todos los ordenadores de una red deben utilizar protocolos estándar para comunicarse.

PROTOCOLO TCP/IP

El Departamento de Defensa de EEUU, preocupado por el corte de la comunicación en una guerra, crea un sistema de información basado en la unión de todos sus puntos de comunicación por varios destinos distintos. De esta forma, si se corta un punto el resto siguen comunicados por otros. Para unir los distintos puntos utilizan la red telefónica y así nace ARPANET (Advanced Research Project Agency Network) en 1970.

En 1974 nace el protocolo TCP/IP y en 1980 el Departamento de Defensa de EEUU decide desclasificar este protocolo como secreto militar. Unix incluye gratuitamente el código TCP/IP para su uso en universidades, lo cual lleva al crecimiento vertiginoso de la hoy conocida como red mundial o red de redes.

TCP/IP no es propiedad de ninguna empresa ni organismo. Todas las particularidades y evoluciones se describen en documentos públicos denominados RFC (Request for Comments) y numerados por orden de aparición. Estas características y posibilidades están convirtiendo a TCP/IP en un protocolo universal.

El protocolo TCP/IP se compone de dos protocolos:

- **Protocolo TCP (Transmission Control Protocol).**

  Es el que asegura que los datos son transmitidos correctamente. Está orientado a la transmisión y controla si la información llega en orden (si no llega ordenada, la ordena), si hay errores, etc.

- **Protocolo IP (Internet Protocol).**

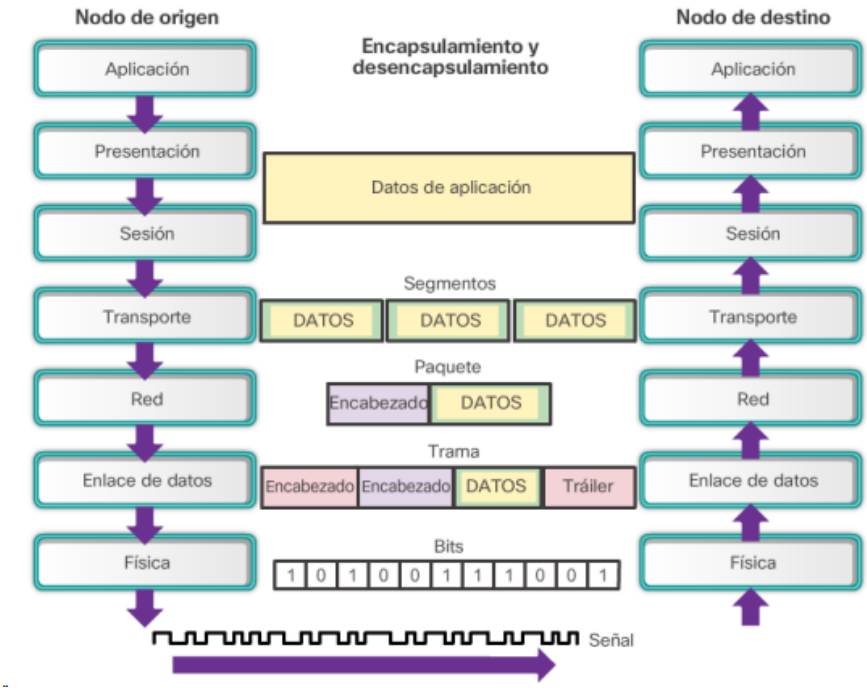
  Permite que las aplicaciones se ejecuten independientemente del hardware que se esté utilizando, tanto a nivel local como en la red. Proporciona un sistema de entrega de paquetes no fiable.

Todo esto implica que, mediante el protocolo TCP/IP, se pueden conectar ordenadores de diferentes tipos, con distinto hardware y con distintos sistemas operativos, tanto en redes de área local como en redes con equipos conectados a larga distancia.

El funcionamiento del protocolo TCP/IP se realiza según el estándar OSI (Open System Interface), que consiste en la transmisión de datos por niveles. Para poder controlar la transmisión, cada nivel incorpora al nivel siguiente su propia cabecera. Cuando la información llega a su destino, la comunicación entre niveles se realiza de forma inversa, quitando las cabeceras recibidas y comprobando que la transmisión es correcta.

MODELO OSI DE ISO

Los siete niveles o capas del modelo OSI son los siguientes:



- **CAPA FÍSICA**

Define el modo de transmisión y de propagación de las señales. Se inicia en la tarjeta de red y se propaga a través de cables y demás soportes.

Las señales pueden ser eléctricas, electromagnéticas u ópticas.

- **CAPA DE ENLACE**

En este nivel los datos digitales se traducen en señales a las que se añaden elementos para formar tramas o paquetes.

Algunos elementos que se añaden son las direcciones físicas del emisor y del destinatario, que hacen referencia a las tarjetas de red.

- **CAPA DE RED**

En este nivel se realiza un proceso que se denomina enrutamiento, consistente en la elección del mejor itinerario para transmitir el paquete en caso de que exista más de una ruta.

La elección se calcula en base a distintos parámetros, como pueden ser el número de redes que se va a atravesar, la duración del transporte, el coste de la comunicación, la saturación de la línea, etc.

- **CAPA DE TRANSPORTE**

Se encarga de comprobar la transmisión correcta de los paquetes entre los emisores y los receptores.

En este nivel se encuentra el protocolo TCP.

• CAPA DE SESIÓN

Esta capa gestiona la recuperación de la comunicación en caso de incidentes.

• CAPA DE PRESENTACIÓN

Se encarga de resolver los problemas asociados con la representación de la información entre los diferentes nodos: juegos de caracteres, caracteres de control, compresión de datos, etc. En este nivel actúa el lenguaje HTML.

• CAPA DE APLICACIÓN

Este nivel constituye la interfaz de comunicación con el usuario. La interfaz puede actuar como un software específico (navegadores, gestores de correo electrónico, etc.) o como comandos del sistema operativo (ftp, telnet, etc.).

PRINCIPALES PROTOCOLOS Y SERVICIOS UTILIZADOS EN INTERNET:

- **Protocolo IPv4 (Internet Protocol).**

El protocolo IP proporciona un sistema de entrega de paquetes no fiable. Gestiona direcciones lógicas que se denominan direcciones IP. Actúa en la capa de red.

Una dirección IP es una dirección lógica de 32 bits, que sirve para identificar cada nodo (equipo) en la red, por lo que cada adaptador de la red dispondrá de su propia dirección IP, que será distinta para cada uno de los nodos.

Las direcciones IP se representan por cuatro bytes, que se escriben separados por un punto (notación decimal puntuada). Cada uno de estos bytes está representado por 8 bits, por lo que su rango de valores oscilará entre 0 y 255.

Las direcciones IP constan de dos campos: un identificador de red (netid), que identifica la red a la que está conectada la estación, y un identificador de host (hostid), que identifica cada host dentro de la red.

En terminología TCP/IP, una red es un grupo de hosts que pueden comunicarse entre sí sin utilizar un encaminador. Todos los hosts TCP/IP que forman una misma red deben tener asignado el mismo identificador de red. Los hosts con distintos identificadores de red deben comunicarse mediante un encaminador.

Dependiendo del número de bits tomados para definir el identificador de red, existen distintas clases de redes, que vienen diferenciadas por el número de redes y de hosts disponibles. Estos valores se indican en la máscara de subred, de forma análoga a las direcciones IP, por lo que tienen 4 bytes y 32 bits. Si un byte tiene el valor 255, indica que dicho byte en la dirección IP se refiere al identificador de red y si tiene el valor 0 indica que dicho byte en la dirección IP se refiere al identificador de host. Las clases de redes son las siguientes:

- **CLASE A.**

  Contiene el valor 255.0.0.0. Esta máscara de subred indica que el primer byte de la dirección IP se destina al identificador de red. Este byte sólo puede contener un valor comprendido entre 1 y 126. Los restantes 3 bytes se destinan al identificador de host. Por lo tanto, en esta red se pueden definir 256 redes (1 byte = 8 bits = 2^8 = 256) y 16.777.216 estaciones (3 bytes = 24 bits = 2^24 = 16.777.216). En realidad, en redes de tipo A sólo se admiten 128 redes y no 256, porque, sólo se utilizan los 7 primeros bits y no los 8. El primer bit contiene siempre el valor 0, que indica el tipo de red.

  El rango de direcciones IP disponibles en este tipo de redes es desde **1.0.0.0 hasta 126.0.0.0**.

  Para utilizar direcciones IP de esta clase en una Intranet con salida a Internet se usan las direcciones IP que comiencen por 10, es decir, 10.0.0.0. Estas direcciones IP no existen en Internet.

- **CLASE B**

  Contiene el valor 255.255.0.0. Esta máscara de subred indica que los dos primeros bytes de la dirección IP se destinan al identificador de red. El primer byte sólo puede contener un valor comprendido entre 128 y 191. Los restantes 2 bytes se destinan al identificador de hosts. Por lo tanto, en esta red se pueden definir 65.536 redes (2 bytes = 16 bits = 2^16 = 65.536) y 65.536 estaciones (2 bytes = 16 bits = 2^16 = 65.536). En realidad, en redes de tipo B sólo se admiten 16.384 redes y no 65.536, porque sólo se utilizan los 14 primeros bits y no los 16. Los dos primeros bits contienen el valor 10, que indican el tipo de red.

  El rango de direcciones IP disponibles en este tipo de redes es desde **128.0.0.0 hasta 191.0.0.0**

  Para utilizar direcciones IP de esta clase en una Intranet con salida a Internet se usan las direcciones IP que comiencen por **172.16, es decir, 172.16.0.0**. Estas direcciones IP no existen en Internet.

- **CLASE C**

  Contiene el valor 255.255.255.0. Esta máscara de subred indica que los tres primeros bytes de la dirección IP se destinan al identificador de red. El primer byte sólo puede contener un valor comprendido entre 192 y 223. El byte restante se destina al identificador de hosts. Por lo tanto, en esta red se pueden definir 16.777.216 redes (3 bytes = 24 bits = 2^24 = 16.777.216) y 256 estaciones (1 byte = 8 bits = 2^8 = 256). En realidad, en redes de tipo C sólo se admiten 2.097.152 redes y no 16.777.216, porque sólo se utilizan los 21 primeros bits y no los 24. Los tres primeros bits contienen el valor 110, que identifican el tipo de red.

  El rango de direcciones IP disponibles en este tipo de redes es desde **192.0.0.0 hasta 223.0.0.0.**

  Para utilizar direcciones IP de esta clase en una Intranet con salida a Internet se usan las direcciones IP que comiencen por 192.168, es decir, 192.168.0.0. Estas direcciones IP no existen en Internet.

- **CLASE D**

  Se reservan para mensajes de **multidifusión o broadcast**. En esta máscara de subred no hay porción de red ni porción de host. Se representa por un número entero que identifica un grupo de hosts.

  Cuando un nodo de la red quiere enviar información a otro pero sólo conoce su dirección IP y no conoce su dirección MAC, el protocolo ARP envía un mensaje broadcast solicitando al nodo destino su dirección física. Todos los nodos de la red reciben el mensaje pero sólo responde el que tiene la dirección IP conocida.

  Este mensaje lleva como máscara de subred el valor 255 en la parte de la dirección IP que se refiere a los hosts.

  Así, si una dirección IP tiene el valor 192.124.255.255 quiere decir que se está enviando un mensaje de multidifusión a todos los hosts de la red 192.124.0.0.

- **CLASE E**

  Su uso es experimental. Los cinco primeros bits son 11110.

Actualmente, las direcciones de clase A están agotadas, las direcciones de clase B están disponibles sólo para grandes empresas y las direcciones de clase C son las únicas disponibles, aunque ya son muy escasas. Los proveedores disponen de bloques de direcciones IP para proporcionar a sus clientes. Para disponer de nuevas direcciones IP, se está trabajando sobre la versión 6 de IP, que se denomina IPNG (IP Next Generation).

Todos los equipos tienen una dirección IP local o loopback, que es la 127.0.0.1. Esta dirección IP no se puede asignar a ningún puesto.

La combinación de una dirección IP y la máscara de red nos indica la red a la que está conectado un equipo. Por ejemplo,

- Equipo con IP 192.168.1.110 y máscara de red 255.255.255.0 está conectado a la red 192.168.1.0;
- Equipo con IP 192.168.1.111 y máscara de red 255.255.255.0 está conectado a la red 192.168.1.0;
- Equipo con IP 192.168.2.210 y máscara de red 255.255.255.0 está conectado a la red 192.168.2.0;
- Equipo con IP 192.168.2.211 y máscara de red 255.255.255.0 está conectado a la red 192.168.2.0;
- Equipo con IP 192.168.3.110 y máscara de red 255.255.0.0 está conectado a la red 192.168.0.0;
- Equipo con IP 192.168.3.111 y máscara de red 255.255.0.0 está conectado a la red 192.168.0.0;

- **Protocolo IPv6 (Internet Protocol version 6).**

Aunque el protocolo IPv4 permite direccionar 4.000 millones de dispositivos, muchas de las direcciones no se pueden utilizar debido a su distribución poco eficaz en un momento en el que no podía preverse la explosión de Internet.

El protocolo IPv6 permite direccionar un gran número de dispositivos, ya que las direcciones se codifican en 16 bytes (128 bits) en lugar de los 4 (32 bits) de IPv4. Además, se ha previsto el uso de redes de alta velocidad y el transporte de datos multimedia.

Es necesario reescribir algunos protocolos, como ARP, RARP o ICMP, pero se ha compatibilizado el uso de las dos versiones. De esta forma, se utilizarán conjuntamente en las redes y los programas que funcionan con IPv6 serán compatibles con IPv4.

Direccionamiento IPv6

El número de direcciones IPv6 posibles es de 2128 o bien 1632, con 32 dígitos hexadecimales, cada uno de los cuales puede tomar 16 valores

En muchas ocasiones las direcciones IPv6 están compuestas por dos partes lógicas: un prefijo de 64 bits y otra parte de 64 bits que corresponde al identificador de interfaz, que casi siempre se genera automáticamente a partir de la dirección MAC de la interfaz a la que está asignada la dirección.

- **Protocolo TCP (Transmission Control Protocol).**

Es un protocolo de transporte que asegura un servicio fiable. Es el que asegura que los datos son transmitidos correctamente. Está orientado a la transmisión y controla si la información llega en orden (si no llega ordenada, la ordena), si hay errores, etc. **Actúa en la capa de transporte**.

El protocolo TCP se basa en las direcciones IP para realizar la transmisión y es el principal usuario del protocolo IP.

Al realizar el control de los datos, la transmisión es más lenta pero se libera a las aplicaciones que utilizan los servicios de TCP del control de la integridad de los datos.

- **Protocolo UDP (User Datagram Protocol).**

Es un protocolo de transporte no fiable. También utiliza el protocolo IP. El control de la integridad de los datos lo realiza la aplicación que use los servicios de UDP. **Actúa en la capa de transporte.**

Al no realizar ningún tipo de control, es más rápido que TCP.

Se utiliza en Internet para transmitir sonido en directo hasta ciertas emisoras de radio. En estas emisiones no es necesario una transmisión perfecta, por eso se utiliza el protocolo UDP.

- **Protocolo DHCP (Dynamic Host Configuration Protocol).**

Permite asignar direcciones IP de forma dinámica. De esta forma, la administración de las direcciones IP la realiza este protocolo y no es posible duplicar una misma dirección IP en varios equipos. Es muy útil cuando a una red se conectan equipos portátiles.

Actúa en la capa de aplicación.

- **Protocolo FTP (File Transfer Protocol).**

Es un protocolo de transferencia de ficheros basado en el protocolo fiable TCP. **Actúa en la capa de aplicación.**

La transferencia de ficheros se puede realizar entre equipos con distintos sistemas operativos.

Cuando un cliente FTP se conecta con un servidor FTP, puede ver la estructura de directorios del servidor, mover archivos, borrar archivos, copiar archivos, etc., siempre dependiendo de los permisos establecidos en el propio servicio FTP y en el servidor FTP a nivel local. Se accederá al servidor FTP autentificando un usuario existente. El servidor se puede configurar para que se acceda con el usuario anonymous, de este modo no es necesario tener creado un usuario concreto en el servidor.

- **Protocolo TFTP (Trivial FTP).**

Actúa igual que el protocolo FTP pero la descarga se realiza más rápidamente y no asegura la integridad de los datos. Esto es debido a que utiliza el protocolo UDP.

- **Protocolo HTTP (Hyper Text Transfer Protocol).**

HTTP es, primeramente, un protocolo de transferencia de archivos. **Actúa en la capa de aplicación.**

En segundo lugar, hace referencia a SGML (Standard General Markup Language), que especifica un lenguaje de definición de datos en forma de enlaces jerárquico (hipertexto). Este lenguaje consta de unos códigos particulares (TAG HTML) que indican al navegador el significado del documento HTML (encabezado, enlaces, imágenes, etc.) y la forma de implementarlo.

HTTP permite un acceso a la información en modo consulta.

Cuando hay que realizar operaciones de cifrado, se utiliza HTTPS, que es una versión ampliada de HTTP.

- **Servicio DNS (Domain Name System).**

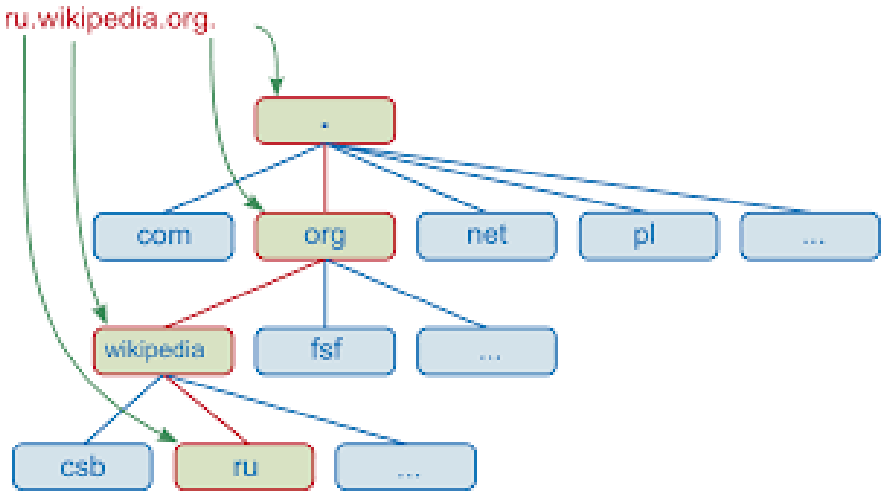
Convierte direcciones IP en nombres de dominios, asociando cada dirección IP con un nombre de dominio. Para realizar esta operación, el servicio DNS gestiona una base de datos que incluye direcciones IP y sus nombres de dominio asociados.

A nivel mundial, los servidores DNS están organizados jerárquicamente. En el primer nivel de esta jerarquía existen 17 servidores DNS, desde los que se pueden acceder a otros servidores DNS de niveles inferiores que gestionan los tipos de organización y los sufijos del país.

Las diferentes partes del nombre de un dominio también han de ir separadas entre sí por un punto.

Por ejemplo: ru.wikipedia.org

Los niveles jerárquicos se ordenan jerárquicamente de izquierda a derecha, es decir los niveles superiores son los de la derecha:



Programas de aplicación, como por ejemplo los navegadores, sólo solicitarán al usuario, en caso de ser necesario, el nombre de dominio de un ordenador con el que establecer una conexión. Entonces, para que la conexión pueda producirse efectivamente a través de uno de los protocolos TCP-IP, es necesario traducir ese nombre a la dirección IP que conduce a ese ordenador. Para esto, existen ordenadores especiales que contienen un software llamado "Servidor DNS", que tiene una base de datos que relaciona cada dirección IP con su nombre de dominio.
Naturalmente, es imposible un servidor de nombres conozca todos los nombres de dominio con sus correspondientes direcciones IP. Por tanto, de acuerdo con la jerarquía de nombres establecidas, las peticiones dirigidas al servidor de nombres se pueden desviar a otro servidor. Este procedimiento, bastante complejo, se conoce como "domain name lookup", o búsqueda del nombre del dominio. En los casos más difíciles, pueden transcurrir varios segundos hasta llegar a averiguar la dirección IP necesaria.

- **Servicio WINS (Windows Internet Name Service).**

En Windows los nombres de los ordenadores que intervienen en una red se denominan NetBIOS. Cada nombre NetBIOS se asocia a una dirección IP. El servicio WINS se encarga de gestionar la base de datos en la que están asociados los nombres NetBIOS y sus direcciones IP.

• Servicio WWW (World Wide Web).

Se compone de millones de sitios que disponen de una dirección IP y de un nombre de dominio. Para acceder a ellos, se escribe una URL (Uniform Resource Locator) que ejecuta el protocolo HTTP.

Este servicio utiliza el protocolo TCP para transmitir los datos informáticos. Para mejorar su velocidad, en el

caso del vídeo y del sonido utiliza el protocolo UDP.

Para realizar transferencias protegidas, tales como los números de las tarjetas de crédito, se utiliza el sistema de protección SSL de cifrado de datos. Las operaciones de cifrado sólo pueden llevarse a cabo en sitios especializados cuya URL comienza por HTTPS.

- **Servicio NFS (Network File System).**

Fue desarrollado por Suns en 1985. Es un sistema de archivos distribuido en entorno heterogéneo. Permite a los usuarios de ordenadores con sistemas operativos distintos acceder a un sistema de archivos remoto sin tener que aprender nuevos mandatos.

• Protocolo SAMBA.

Es una versión del protocolo SMB de Unix. Permite compartir recursos entre redes heterogéneas e incluso convertir un servidor Unix en controlador de un dominio Windows 2000 con un recurso compartido NETLOGON para descargar los scripts y las directivas del sistema NT.

- **Protocolo Telnet.**

Es un protocolo de emulación de terminal. Se establece una sesión (login) entre un puesto de trabajo (cliente telnet) y una máquina remota (servidor telnet). Cualquier mandato que solicita el cliente se transmite y se ejecuta en el servidor telnet. La salida de la orden se muestra en el cliente telnet. Este proceso requiere que el usuario del equipo cliente telnet conozca el sistema operativo del servidor telnet.

Actúa en la capa de aplicación.

- **Protocolo ICMP (Internet Control error Message Protocol).**

Funciona junto con el protocolo IP para proporcionar a TCP controles e información sobre errores, ya que IP no detecta ninguna anomalía que se pueda producir. **Actúa en la capa de red.**

Este protocolo es utilizado por los enrutadores, a fin de especificar un cierto número de eventos importantes.

Algunos mensajes de error que genera este protocolo son: Timeout Exceeded, Destination Unreachable, etc.

- **Protocolo ARP (Address Resolution Protocol).**

Permite determinar la dirección MAC de un nodo a partir de su dirección IP. La resolución inversa la lleva a cabo el protocolo RARP (Reverse Adress Resolution Protocol). **Actúa en la capa de red.**

- **Protocolo RIP (Routing Internet Protocol).**

Este protocolo permite el intercambio de información entre los enrutadores, de forma que cada uno de ellos pueda disponer de la lista de todas las redes. Este proceso se denomina enrutamiento dinámico.

Actúa en la capa de aplicación.

- **Protocolo SMTP (Simple Mail Transfer Protocol).**

Es un protocolo de transferencia simple utilizado en mensajería electrónica y basado en UDP e IP. Permite adjuntar archivos informáticos a los mensajes.

Actúa en la capa de aplicación.

Las direcciones de correo electrónico se componen de una referencia a la persona seguida del nombre de dominio en el que está ubicada la cuenta de correo. Ambas se separan por el carácter @.

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

Gestiona el nombre de usuarios estándares de las cuentas de correo.

- **Protocolo SNMP (Simple Network Management Protocol).**

Es un protocolo basado en UDP que permite administrar a distancia dispositivos y programas. **Actúa en la capa de aplicación.**

Este protocolo recoge la información de los encaminadores, puentes o aplicaciones específicas, mostrar estadísticas y enviar órdenes a los dispositivos con el fin de gestionar de forma remota los eventos que se produzcan.

- **Protocolo PPTP (Point to Point Tunneling Protocol).**

Este protocolo simula una red privada entre dos puntos de una red pública. El interés de este protocolo radica en que permite establecer conexiones seguras en una red pública, principalmente en Internet. Se utiliza, entre otras aplicaciones, para el desarrollo de conexiones de empresa hacia la red mundial.

- **Protocolo NETBEUI (NetBIOS Extended User Interface).**

NetBIOS (Network Basic Input/Output System). Fue introducido por IBM en 1985 y optimizado para el uso de pequeñas redes y de archivos compartidos. NetBIOS fue adoptado por Microsoft y creó la versión extendida NetBEUI para sus propios sistemas operativos.

Su función es convertir los nombres de ordenadores en direcciones MAC, sin utilizar direcciones lógicas o direcciones IP. Por esta razón, no es enrutable.

La resolución a dirección MAC la realiza el propio puesto, que envía un mensaje de multidifusión (broadcast) sobre la red. Cada estación mantiene una tabla de relaciones entre los nombres NetBIOS y las direcciones MAC de todos los equipos de la red.

Este protocolo utiliza poca memoria pero consume mucho ancho de banda debido a los mensajes de

multidifusión.

Para referirse a una estación desde la línea de comandos o desde una aplicación, se utiliza el formato **\\NombreDeEstación.**

La simplicidad de este protocolo y el hecho de consumir pocos recursos, hace que sea muy utilizado, actualmente, por los productos Microsoft, IBM y Novell.

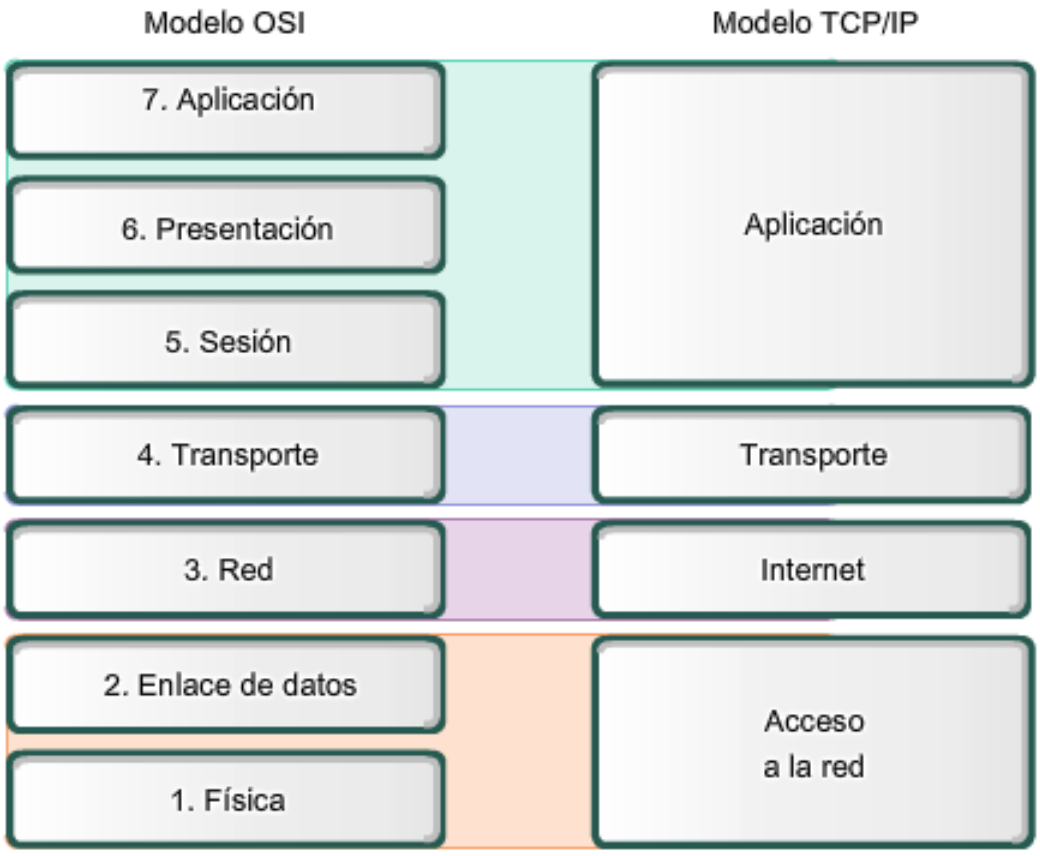
- **Protocolo PPP (Point to Point Protocol).**

Proporciona diversas funciones, como el control de errores, la seguridad, la asignación dinámica de dirección IP y el soporte de diversos protocolos LAN, como IP, IPX, AppleTalk o NetBEUI.

- **Protocolo RDP (Remote Desktop Protocol).**

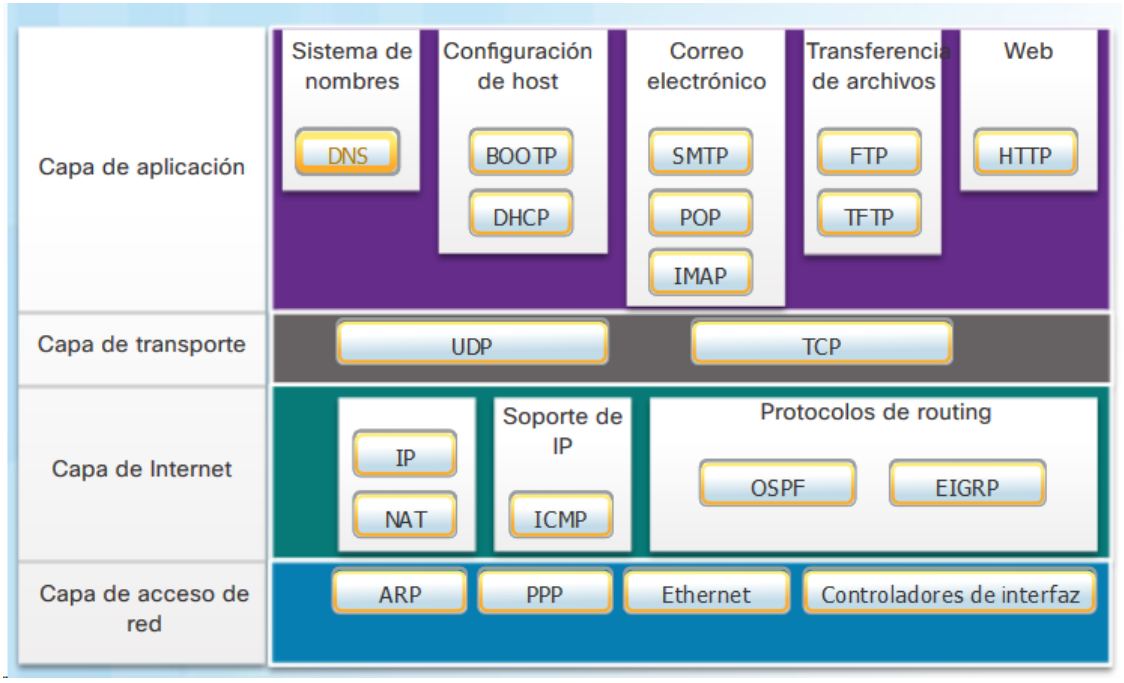
Cuando un cliente se conecta a un servidor utilizando este protocolo, todos los procesos lanzados por el cliente se ejecutan en el servidor y al cliente sólo se envían los resultados de los procesos. Este protocolo es el que utiliza el servicio Terminal Server de Windows. Su cliente es el Escritorio Remoto de Windows.

COMPARACIÓN Modelo OSI y Modelo TCP/IP



Las semejanzas claves están en la capa de red y de Transporte.

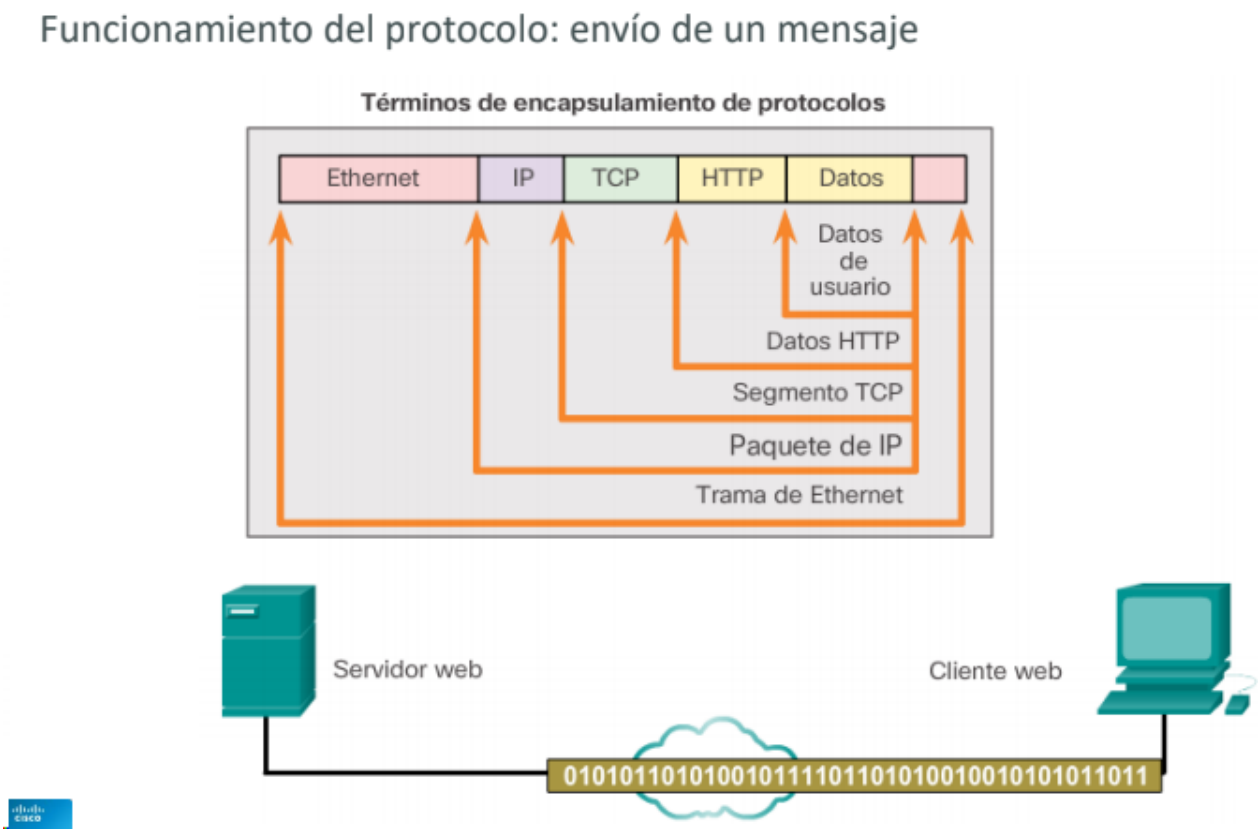
CONJUNTO DE PROTOCOLOS TCP/IP



Los protocolos individuales se organizan en capas mediante el modelo de protocolo TCP/IP: aplicación, transporte, Internet y capas de acceso a la red. Los protocolos TCP/IP son específicos de las capas Aplicación, Transporte e Internet. Los protocolos de la capa de acceso a la red son responsables de la entrega de los paquetes IP en los medios físicos. Estos protocolos de capa inferior son desarrollados por organizaciones de estandarización, como el IEEE.

La suite de protocolos TCP/IP se implementa como una pila de TCP/IP tanto en los hosts emisores como en los hosts receptores para proporcionar una entrega completa de las aplicaciones a través de la red. Los protocolos Ethernet se utilizan para transmitir el paquete IP a través de un medio físico que utiliza la LAN.

PROCESO DE COMUNICACIÓN



1. Supongamos el ejemplo anterior en el que el servidor web está preparando la **página HTML como los datos** que se van a enviar.

2. El **encabezado HTTP** del protocolo de aplicación se agrega al frente de los datos HTML. El encabezado contiene diversos tipos de información, incluida la versión de HTTP que utiliza el servidor y un código de estado que indica que tiene información para el cliente web.

3. El protocolo de capa de aplicación HTTP entrega los datos de la página web con formato HTML a la capa de transporte. **El protocolo de la capa de transporte TCP se utiliza para administrar conversaciones individuales,** en este ejemplo entre el servidor web y el cliente web.

4. Luego, la información IP se agrega al frente de la información TCP. **IP asigna las direcciones IP de origen y de destino** que corresponden. Esta información se conoce como paquete IP.

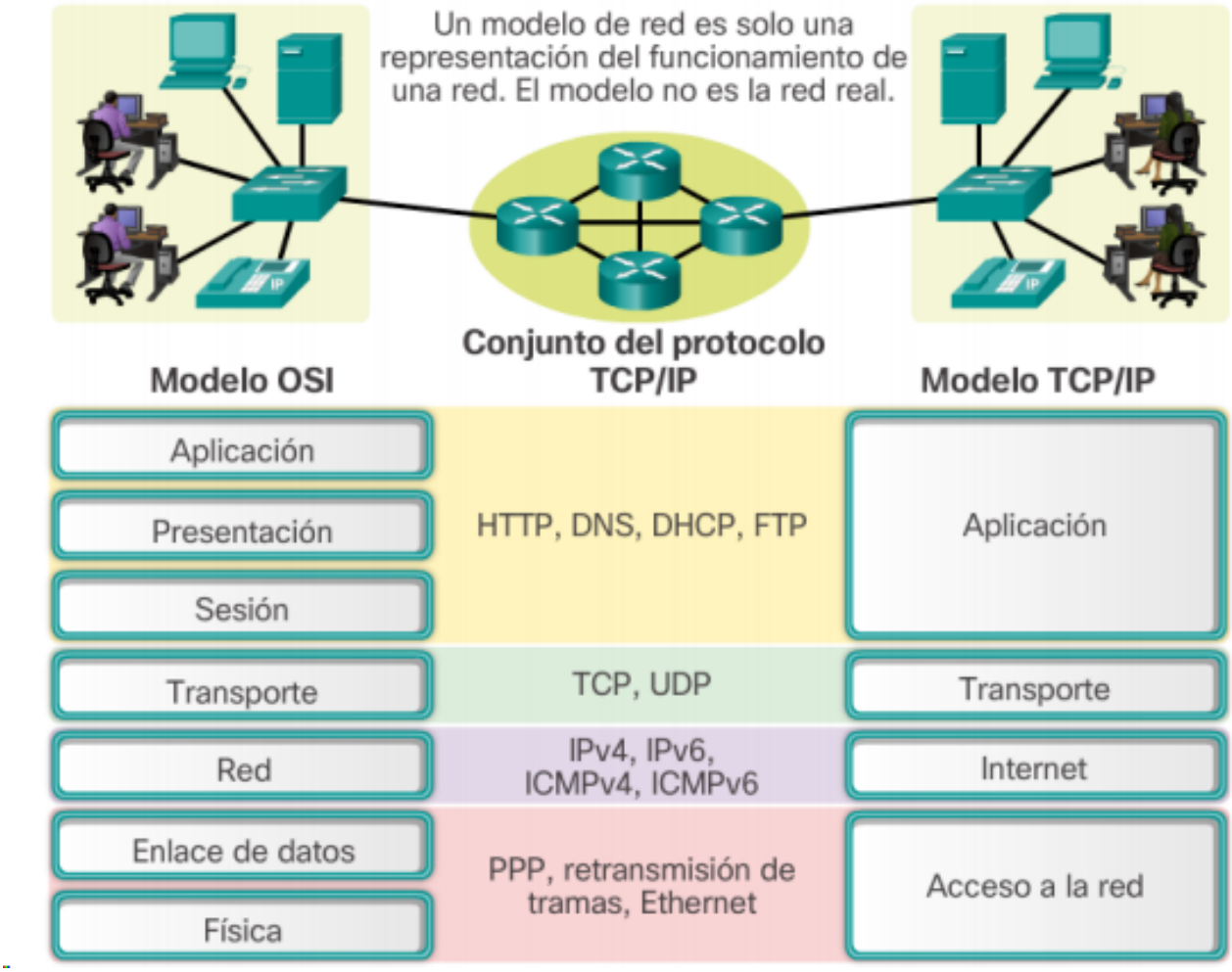
5. El protocolo **Ethernet** agrega información en ambos extremos del paquete IP, conocidos como la “trama de enlace de datos”. **Esta trama se envía al router más cercano a lo largo de la ruta hacia el cliente web. Este router elimina la información de Ethernet, analiza el paquete IP, determina el mejor camino para el paquete, coloca el paquete en una trama nueva y lo envía al siguiente router vecino hacia el destino.** Cada router elimina y agrega información de enlace de datos nueva antes de reenviar el paquete.

6. Estos datos ahora se transportan a través de la red, que consta de medios y dispositivos intermediarios.

7. Cuando el cliente que recibe las tramas de enlace de datos que contienen los datos. **Cada encabezado de protocolo se procesa y luego se elimina en el orden inverso al que se agregó.** La información de Ethernet se procesa y se elimina, seguida por la información del protocolo IP, luego la información de TCP y, finalmente, la información de HTTP.

8. A continuación, la información de la página web se transfiere al software de navegador web del cliente.

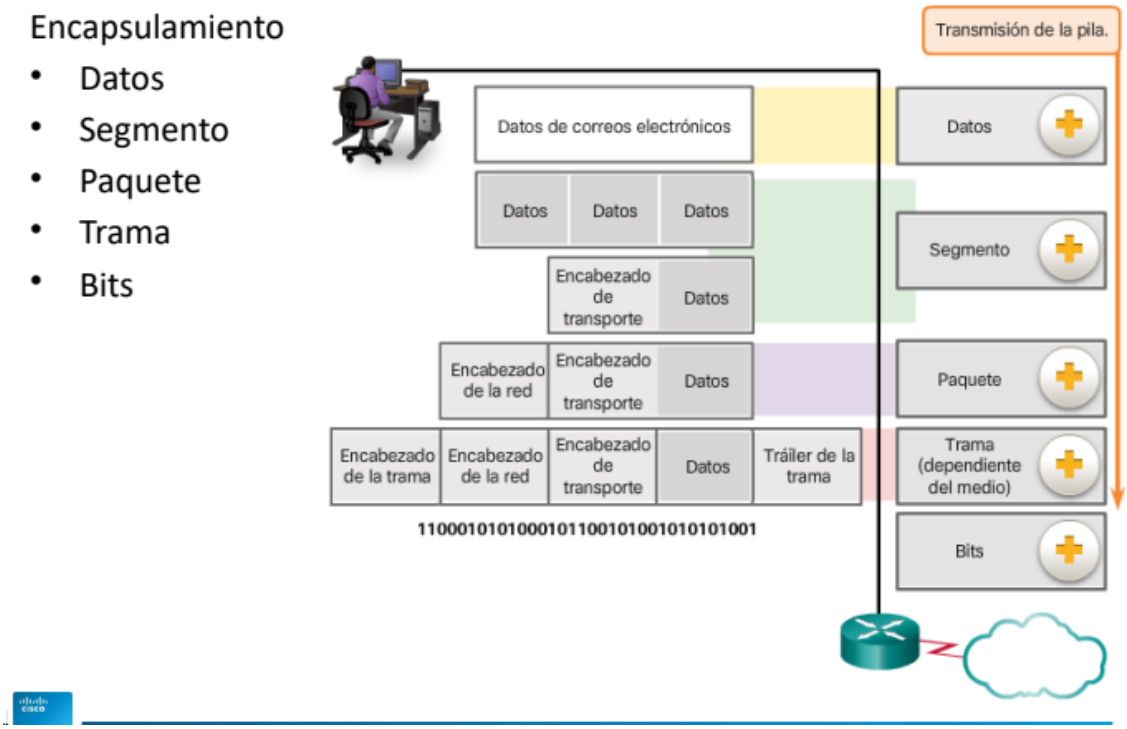
BENEFICIOS DEL USO DE UN MODELO POR CAPAS



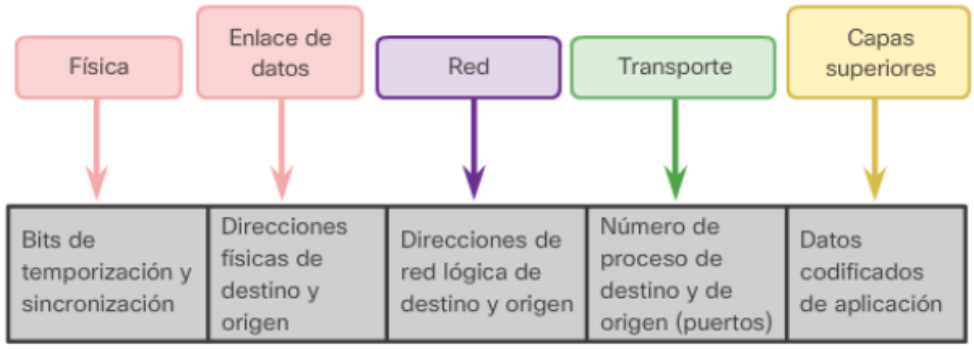
Los beneficios por el uso de un modelo en capas para describir protocolos de red y operaciones son:

- Ayuda en el diseño de protocolos, ya que los protocolos que operan en una capa específica tienen información definida según la cual actúan, y una interfaz definida para las capas superiores e inferiores.
- Fomenta la competencia, ya que los productos de distintos proveedores pueden trabajar en conjunto.
- Evita que los cambios en la tecnología o en las funcionalidades de una capa afecten otras capas superiores e inferiores.
- Proporciona un lenguaje común para describir las funciones y capacidades de red.

ENCAPSULAMIENTO DE LOS DATOS. UNIDADES DE DATOS DE PROTOCOLO



DIRECCIONES DE RED Y DE ENLACE DE DATOS



La capa de red y la capa de enlace de datos son responsables de enviar los datos desde el dispositivo de origen o emisor hasta el dispositivo de destino o receptor.
Los protocolos de las dos capas contienen las direcciones de origen y de destino, pero sus direcciones tienen objetivos distintos.

- **Direcciones de origen y de destino de la capa de red:** son responsables de enviar el paquete IP desde el dispositivo de origen hasta el dispositivo final, ya sea en la misma red o a una red remota.
- **Direcciones de origen y de destino de la capa de enlace de datos:** son responsables de enviar la trama de enlace de datos desde una tarjeta de interfaz de red (NIC) a otra en la misma red.

PUERTO DE RED

Un puerto de red es una interfaz para comunicarse con un programa a través de una red.
Un puerto suele estar numerado. La implementación del protocolo en el destino utilizará ese número para decidir a qué programa entregará los datos recibidos. Esta asignación de puertos permite que una máquina establecer simultáneamente diversas conexiones con máquinas distintas, ya que todos los paquetes que se reciben tienen la misma dirección, pero van dirigidos a puertos diferentes.

Los números de puerto se indican mediante una palabra, 2 bytes (16 bits), por lo que existen 65535.
La IANA (Internet Assigned Numbers Authority) es la encargada de la asignación de los puertos. Creó tres categorías:

- **Puertos bien conocidos:** Los puertos inferiores al 1024 son puertos reservados para el sistema operativo y usados por "protocolos bien conocidos" como por ejemplo HTTP (servidor Web), POP3/SMTP (servidor de e-mail) y Telnet. Si queremos usar uno de estos puertos tendremos que arrancar el servicio que los use teniendo permisos de administrador.
- **Puertos registrados**: Los comprendidos entre 1024 (0400 en hexadecimal) y 49151 (BFFF en hexadecimal) son denominados "registrados" y pueden ser usados por cualquier aplicación. Existe una lista pública en la web del IANA donde se puede ver qué protocolo usa cada uno de ellos.
- **Puertos dinámicos o privados:** Los comprendidos entre los números 49152 (C000 en hexadecimal) y 65535 (FFFF en hexadecimal) son denominados dinámicos o privados, normalmente se asignan en forma dinámica a las aplicaciones de clientes al iniciarse la conexión. Se usan en conexiones peer to peer (P2P).

NIVEL DE APLICACIÓN EN TCP/IP. PROTOCOLOS Y PUERTOS

La capa de nivel de aplicación es la ubicada en la parte superior de la jerarquía del TCP- IP
Hay muchos protocolos de nivel de aplicación, se crean nuevos cada día y la mayoría proveen servicios directos a los usuarios.
Los básicos son:

PROTOCOLO	ENTIDAD DE TRANSPORTE	PUERTO	DESCRIPCIÓN
FTP	TCP	21	Transferencia de archivos
SSH	TCP/UDP	22	Terminal de red cifrado
Telnet	TCP	23	Terminal de red
SMTP	TCP	25	Envío de correos electrónicos
DHCP	TCP	67 y 68	Protocolo de Asignación de IP Dinámica
TFTP	UDP	69	Transferencia de archivos

HTTP	TCP	80	www
POP3	TCP	110	Descarga de correos electrónicos
RPC	TCP/UDP	111	Llamada a procedimiento remoto
SFTP	TCP	115	Transferencia de ficheros seguro
NTP	UDP	123	Tiempo sincronizado
IMAP4	TCP	143 220 993	Descarga de correos electrónicos
LDAP	TCP	389	Protocolo de acceso ligero a datos
HTTPS	TCP	443	www seguro
SMTPS	TCP	465	Correo seguro
RIP	UDP	520	Routing Information Protocol (Protocolo de Información de Enrutamiento)
SQL SERVER	TCP/UDP	1433	Bases de datos
NFS	TCP/UDP	2049	Sistemas de ficheros en red
MYSQL	TCP	3306	Bases de datos
RDP	TCP	3389	Remote Desktop Protocol (Escritorio Remoto)
VNC	TCP	5400 5500 5600 5700 5800	Escritorio remoto por VNC
X-WINDOW	TCP/UDP	6000+n	Servidor de X-Windows
HTTP alternativo	TCP	8080	HTTP alternativo al puerto 80. Ej. Tomcat lo usa como puerto por defecto.

y otros.....

Número de puerto: Cada protocolo de aplicación TCP-IP tiene asignado un número de puerto, se trata de números lógicos que identifican determinadas aplicaciones de Internet especiales dentro del entorno del TCP-IP, que no tienen nada que ver con el hardware a través del cual se realiza la comunicación con Internet.