# Redes e internet

## ¿Qué es una red?

Es un conjunto de ***computadoras interconectadas*** de modo que puedan compartir archivos de datos, programas, impresoras y otros recursos.

En general esas computadoras están conectadas a uno o más **servidores,** que son PC con recursos y programas específicos para funcionar como tales. Esos servidores son los que almacenan la información común y controlan los periféricos a compartir.

El resto de las computadoras personales, que no son servidores, se denominan **clientes** y trabajan dentro del "dominio" de estos servicios.

Esta estructura de ordenadores **"CLIENTE-SERVIDOR"** es lo que se conoce como una red de ordenadores.


La idea tiene sus orígenes en los entornos corporativos financieros de los años 70 del siglo pasado, en Estados Unidos. Era una época de grandes supercomputadoras, capaces de generar millones de instrucciones por segundo, pero limitadas a una habitación e incomunicadas con el resto del mundo. En los bancos y otras instituciones financieras, el uso de computadoras comenzó a hacerse habitual, sobre todo con la explosión de los equipos IBM destinados a fines comerciales. Las primeras experiencias de redes de gran cobertura son de finales de la década del 60 y principios de los 70.

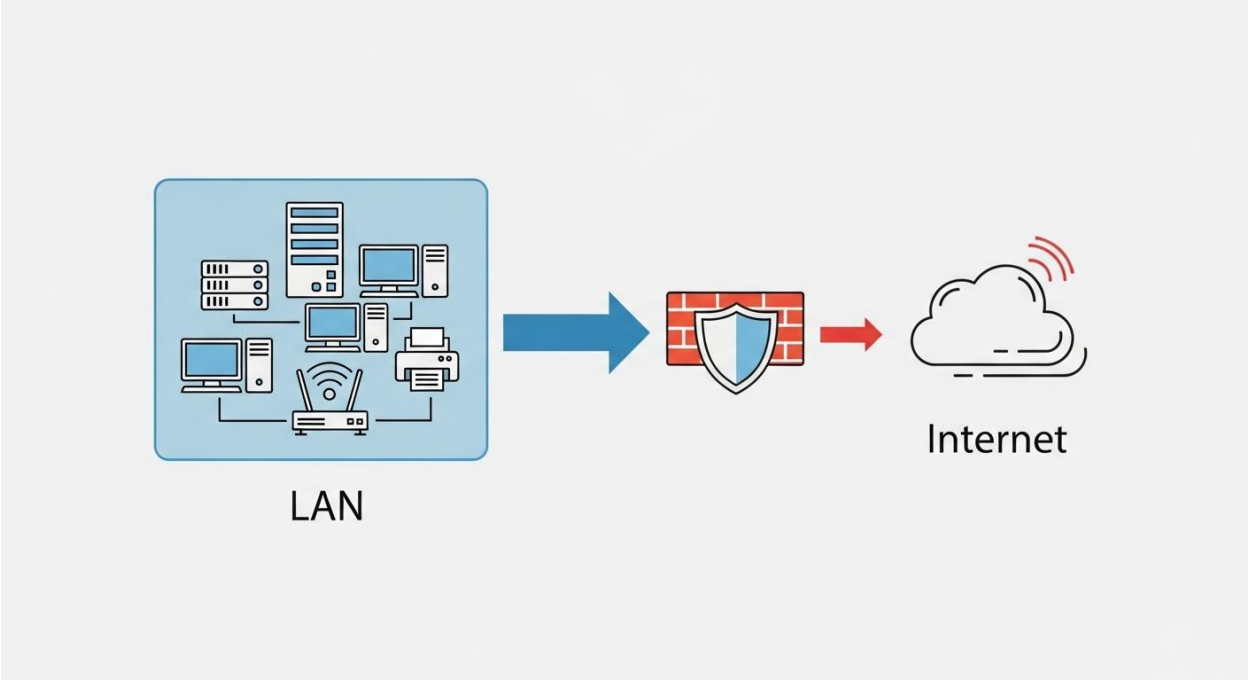
Allí surge la idea de generar computadoras, cuya función no sea la de procesar datos o calcular fórmulas, sino la de recibir y enviar información a equipos que estén conectados entre si. Estas computadoras se denominaron "servidores" y se encargaban de centralizar archivos y documentos para luego entregarlos a las máquinas conectadas, denominadas "clientes". Este concepto es la base del funcionamiento de Internet y de la informática corporativa en millones de empresas de todo el mundo, que pueden centralizar y optimizar recursos, espacio en discos y minimizar el tráfico de datos entre personas.

Un programa de ordenador se especializa en recoger y presentar información (el cliente) y otro en hacer que esta información sea fácilmente accesible (el servidor). Sus principales características son:
Los servidores corren programas que, por lo general, se ejecutan en ordenadores con características especiales (en cuanto a su sistema operativo, potencia, etc.). Cada uno de ellos tiene una información que proporcionar; para obtenerla, se llama al ordenador que la ofrece, y se establece un diálogo con el programa correspondiente. A través de este diálogo, es posible conocer la información que está disponible, y recoger lo que interesa.
Los clientes son programas que facilitan el acceso a los servidores; conocen las características del diálogo con cada tipo de servicio, y gestionan todos los pasos a seguir para recoger y mostrar la información deseada. Normalmente se ejecutan en ordenadores personales, PC's, Macintosh.

## Tipos de redes:

**RED DE ÁREA AMPLIA - WAN.** (*Wide Area Network)*, es un tipo de red de computadoras capaz de cubrir distancias desde unos 100 hasta unos 1000 km. Un ejemplo de este tipo de redes sería, Internet. Muchas WAN son construidas por y para una organización o empresa particular y son de uso privado, otras son construidas por los proveedores de internet (ISP) para proveer de conexión a sus clientes.

Hace unos años atrás las conexiones WAN se realizaban punto a punto, donde, por cada sitio al cual se necesitaba acceder, se creaban circuitos/conexiones virtuales estáticas para permitir las comunicaciones, tanto de voz como de datos.




Por Ejemplo: Un negocio de venta de electrodomésticos con una casa central y 9 sucursales, si se quisiera conectar cada sucursal solo con la casa central, debería generar 9 conexiones, entre Casa

Central y cada una de las sucursales, esta topología se denomina estrella, donde el centro de la estrella es Casa Central, en este tipo de arquitectura todas las comunicaciones pasan por casa central, es decir, que si una sucursal necesita comunicarse con otra debe hacer tránsito – se denomina así al camino que debe realizar un paquete de datos- indefectiblemente por casa central.

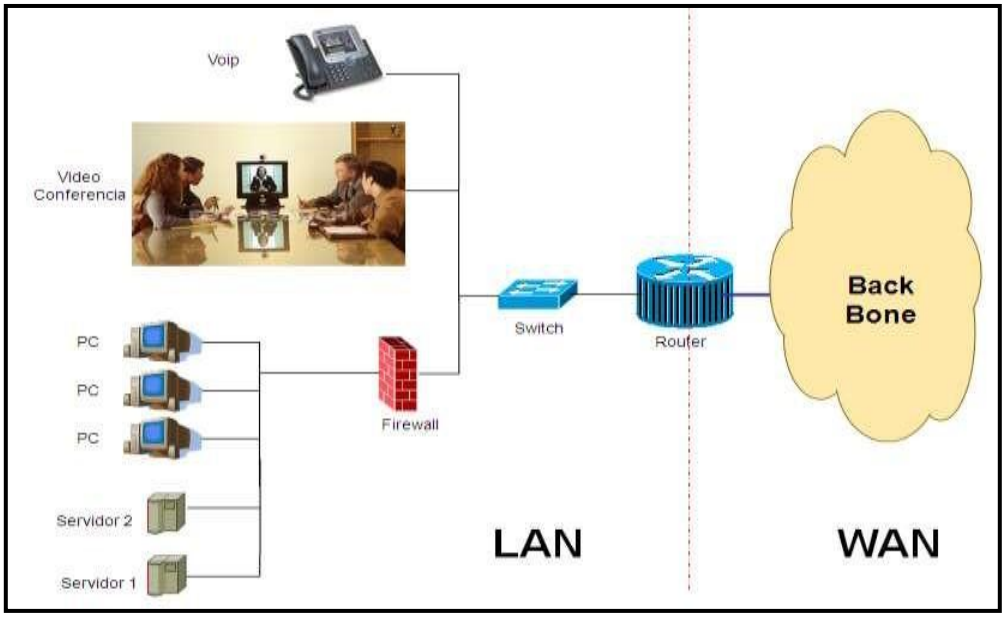
En el caso de pretender que cada sitio tenga comunicación directa con el resto de los puntos, tomando el ejemplo anterior (9 sucursales y una Casa Central), se deberían crear 90 conexiones virtuales, esta arquitectura se denomina malla completa o FullMesh, donde todos se ven con todos.

En la actualidad esto se simplificó con la implementación de protocolos de ruteo en routers de los backbones (Centro) de Wan. En estos protocolos se especifica solo las direcciones IPs de cada sucursal y el protocolo se encarga de direccionar las comunicaciones sin necesidad que estas lleguen a procesarse en la casa central, esto incrementa la capacidad de inteligencia en los backbones.

Normalmente un vínculo de WAN tiene una conexión física a un punto de acceso a un backbone. Las redes WAN pueden usar sistemas de comunicación vía satélite o de radio.

**RED DE ÁREA LOCAL – LAN.** (Local Área Network) es la interconexión de varias computadoras y periféricos. Su extensión está limitada físicamente a un edificio o a un entorno de 200 metros, con repetidores podría llegar a la distancia de un campo de 1 kilómetro. Su aplicación más extendida es la interconexión de computadoras personales y estaciones de trabajo en oficinas, fábricas, etc.

Las últimas implementaciones han sido, aplicando diferentes técnicas y protocolos, la inclusión de Video Conferencia, Voip (Voz mediante IP), entre otros servicios que requieren gran ancho de banda.




**RED DE ÁREA METROPOLITANA- MAN:** (Metropolitan Area Network) es una red de alta velocidad (banda ancha) que da cobertura en un área geográfica extensa, proporciona capacidad de integración de

múltiples servicios mediante la transmisión de datos, voz y vídeo, sobre medios de transmisión tales como fibra óptica y par trenzado (MAN BUCLE). Las Redes MAN BUCLE, se basan en tecnologías Bonding, de forma que los enlaces están formados por múltiples pares de cobre con el fin de ofrecer el ancho de banda necesario.

El concepto de red de área metropolitana representa una evolución del concepto de red de área local a un ámbito más amplio, cubriendo áreas mayores que en algunos casos no se limitan a un entorno metropolitano sino que pueden llegar a una cobertura regional e incluso nacional mediante la interconexión de diferentes redes de área metropolitana.

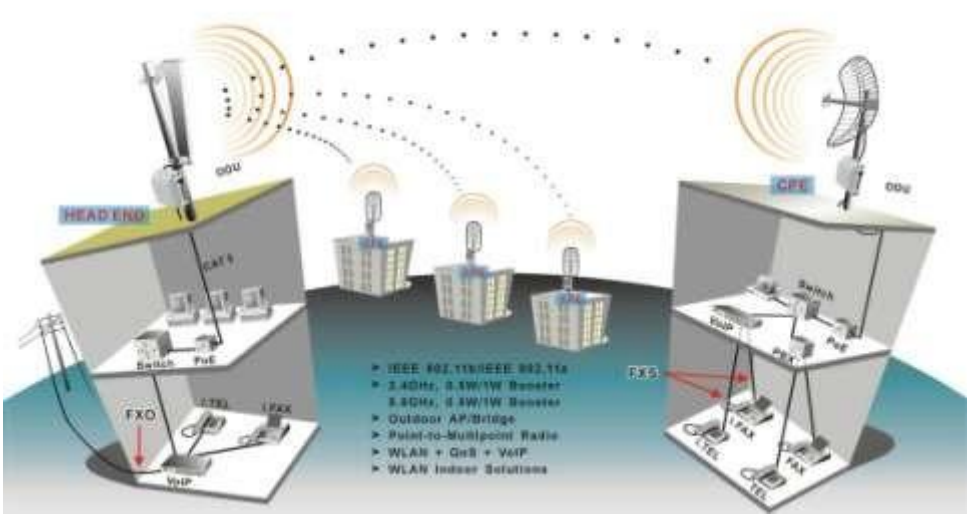
Las redes MAN también se aplican en las organizaciones, en grupos de oficinas corporativas cercanas a una ciudad, estas no contiene elementos de conmutación, los cuales desvían los paquetes por una de varias líneas de salida potenciales. Estas redes pueden ser públicas o privadas.

Las redes de área metropolitana, comprenden una ubicación geográfica determinada "ciudad, municipio", y su distancia de cobertura es mayor de 4 km. Son redes con dos buses unidireccionales, cada uno de ellos es independiente del otro en cuanto a la transferencia de datos.

Las Redes Metropolitanas, permiten la transmisión de tráfico de voz, datos y video con garantías de baja latencia, razones por las cuales se hace necesaria la instalación de una red de área metropolitana a nivel corporativo, para corporaciones que cuentas con múltiples dependencias en la misma área metropolitana.

## RED INALÁMBRICA – WLAN.

(Wireless network) es un término que se utiliza en informática para designar la conexión de nodos sin necesidad de una conexión física (cables), ésta se da por medio de ondas electromagnéticas. La transmisión y la recepción se realizan a través de puertos.



Una de sus principales ventajas es la de los costos, ya que se elimina todo el cableado y conexiones físicas entre nodos, pero también tiene una desventaja considerable ya que para este tipo de red se debe de tener una seguridad mucho más exigente y robusta para evitar a los intrusos.

En la actualidad las redes inalámbricas son una de las tecnologías más prometedoras.

## Existen dos categorías de las redes inalámbricas

**LARGA DISTANCIA:** Son utilizadas para distancias grandes como puede ser otra ciudad u otro país.

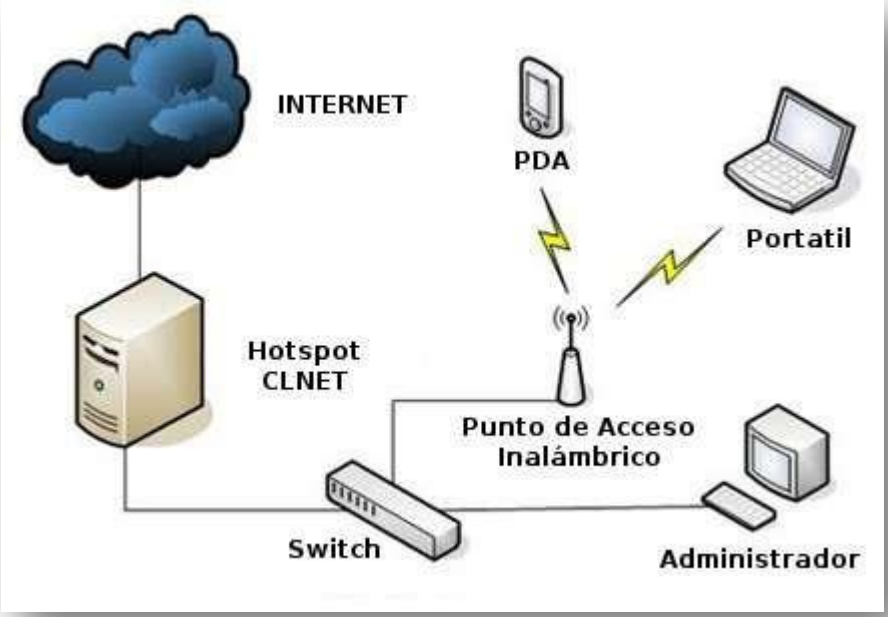
**CORTA DISTANCIA:** Son utilizadas para un mismo edificio o en varios edificios cercanos no muy retirados.

Según su cobertura, se pueden clasificar en diferentes tipos:

# WIRELESS PERSONAL AREA NETWORK

En este tipo de red de cobertura personal, existen tecnologías basadas en HomeRF (estándar para conectar todos los teléfonos móviles de la casa y los ordenadores mediante un aparato central); Bluetooth.

# WIRELESS LOCAL AREA NETWORK




Las redes inalámbricas metropolitanas se basan principalmente en tecnologías de telefonía móvil celular. Si bien en su momento se propusieron estándares como WiMAX, fueron las redes 4G (LTE) y, más recientemente, 5G, las que se consolidaron para ofrecer conectividad de banda ancha en grandes áreas geográficas. Estas tecnologías no solo dan servicio a teléfonos móviles, sino que también se utilizan para el Acceso Fijo Inalámbrico (FWA), llevando internet de alta velocidad a hogares y empresas, y son la base para el ecosistema del Internet de las Cosas (IoT).

# WIRELESS METROPOLITAN AREA NETWORK

Para redes de área metropolitana se encuentran tecnologías basadas en WiMAX (Worldwide Interoperability for Microwave Access, es decir, Interoperabilidad Mundial para Acceso con Microondas), un estándar de comunicación inalámbrica basado en la norma IEEE 802.16. WiMAX (es un protocolo parecido a Wi-Fi, pero con más cobertura y ancho de banda).

# WIRELESS WIDE AREA NETWORK

Una WWAN difiere de una WLAN (wireless local área network) en que usa tecnologías de red celular de comunicaciones móviles como WiMAX (aunque se aplica mejor a Redes WMAN),

UMTS (Universal Mobile Telecommunications System), GPRS, EDGE, CDMA2000, GSM, CDPD,

HSPA y 3G para transferir los datos. También incluye Wi-Fi autónoma para conectar a internet.

## Hardware de red –Componentes de una red.

Hardware de red normalmente se refiere a los equipos que facilitan el uso de una red informática. Típicamente, esto incluye enrutadores (routers), switches, hubs, gateways, tarjetas de interfaz de red, cables de redes, módems, firewalls

**ROUTER:** Enrutador, direcciona los paquetes de información que circulan por la red. Maneja protocolos de ruteo, políticas de Qos(Calidad de servicio) y pueden analizar reglas de seguridad. Por lo general tienen uno o dos puertos que dan servicio de LAN y varios puertos de WAN, también tienen capacidad de brindar servicios de voz a través de puertos analógicos donde se pueden conectar teléfonos estándares, todas estas prestaciones son totalmente acondicionables a las necesidades del cliente. Es uno de los componentes con más inteligencia de la red.

**SWITCH:** Los más utilizados son los switches de capa2, no manejan protocolo de ruteo, solo brindan gran capacidad de conexiones, son los más vistos en un entorno LAN conectados detrás de un router. Las capacidades varían, se presentan switches de 4 hasta más de 50 puertos de conexión.

**GATEWAYS:** Puerta de Enlace. Es un equipo o sistema dentro de un equipo que traduce los protocolos de una red para conectarla a Internet. Enmascara las IP interna y permite a todas las máquinas navegar a través de una misma IP externa o enlace a Internet. Se encargan de acoplar redes dissimiles, por ejemplo: una empresa que brinda servicios de telefoniaIP utiliza Gateways para vincular su red con la red de telefonía pública, digamos que Telecentro (telefoniaIp) necesita gateways para que sus usuarios puedan comunicarse con usuarios de Telecom o Telefónica (telefonía pública).

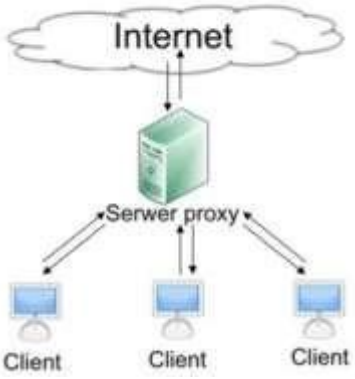

**LAS TARJETAS DE INTERFACE DE RED:** Son las tarjetas que se instalan en las computadoras para poder conectarlas a un medio de comunicaciones.


**FIREWALLS:** Son los equipos que su única utilidad es dar seguridad a la red, esto se realiza mediante tablas que cargadas de determinada forma pueden filtrar programas, paginas, ips por origen o destino, puertos, se pueden aplicar servicios de encryptacion de datos, esto es para evitar ataques a nuestra red o limitar el uso de nuestro sistema a solo determinadas paginas o servicios. Por ejemplo, si deseo que ningún empleado tenga acceso a internet puedo bloquear el puerto 80 en el firewall, el puerto 80 identifica a las conexiones http.

**MODEMS:** **(Modulador-Demodulador):** Es el dispositivo que convierte las señales digitales de tus equipos (computadora, consola, etc.) en un formato analógico compatible con el medio de transmisión del proveedor de internet (fibra óptica, cable coaxial, etc.), y viceversa. Su función es ser el "traductor" que permite la conexión con la red externa. Los tipos más comunes hoy en día son: **Módems de Fibra Óptica (ONT):** Se utilizan en conexiones FTTH (Fiber-to-the-Home) y ofrecen las velocidades más altas del mercado. Convierten las señales eléctricas en pulsos de luz. **Cablemódems:** Operan sobre la red de cable coaxial (la misma de la TV por cable). Son el estándar en muchas zonas urbanas. **Módems**

**DSL:** Funcionan sobre la línea telefónica tradicional, pero ofrecen velocidades de banda ancha muy superiores al antiguo sistema *dial-up*.

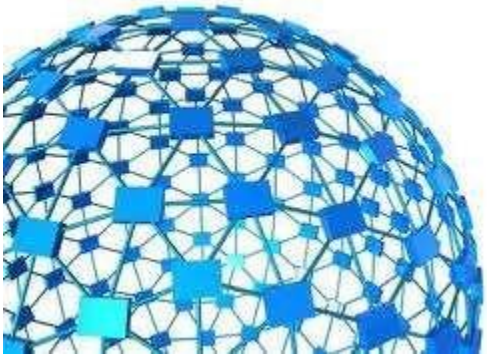
**CABLES DE RED:** Identifican solo el medio físico que utilizamos para conectar cualquiera de nuestros equipos de red, router, switch, pcs, etc.




**PROXY:** Es un programa o dispositivo que realiza una acción en representación de otro

# ¿Qué es Internet?

Es una gran red de redes de computadoras. La palabra significa "inter - red", o "red de redes", porque interconecta varias redes entre sí.
Internet provee de diferentes servicios, que pueden agruparse en:



- La **World Wide Web** (www), que son las páginas que visitamos
- El **Correo Electrónico**
- Los **Grupos de Discusión** o newsgroups y su evolución, las redes sociales.
- La **conexión en tiempo real** (chat, videoconferencia, telefonía por Internet)
- La **televisión IP** (contenido audiovisual a través de la red)

La WWW o **World Wide Web** es un modo de intercambio de información a través de internet distribuida alrededor del mundo mediante servidores web. Utiliza un Protocolo denominado **HTTP:** Hipertext Transfer Protocol, creado por Tim Berners Lee en 1991, junto con el lenguaje **HTML:** Hipertext Markup Language.

## Protocolos, lenguajes y direcciones

Para comunicarnos en Internet necesitamos de **protocolos y lenguajes** que hagan posible el intercambio de información entre computadoras con diferentes sistemas operativos.

También necesitamos **direcciones** para establecer el contacto.

# Protocolos

Son conjunto de reglas establecidas con el propósito de estandarizar el intercambio de información entre equipos informáticos. Al seguir un mismo protocolo se garantiza que habrá compatibilidad entre los dispositivos en los distintos puntos de un sistema informático.

**PROTOCOLO DE ENLACE: ETHERNET.** Estándar para redes de área local

### PROTOCOLO DE TRANSPORTE: IP – INTERNET

**PROTOCOL.** Tiene la función de trasladar información en paquetes, y no está orientado a conectar. No brinda servicio de corrección de errores por lo que no es muy confiable: Si se necesita fiabilidad, ésta es proporcionada por los protocolos de la capa de transporte, como TCP.


### PROTOCOLO DE TRANSPORTE: TCP – TRANSFERENCE

**CONTROL PROTOCOL.** Es la capa intermedia entre el protocolo de internet (IP) y la aplicación. Garantiza que los datos serán entregados en su destino sin errores y en el mismo orden en que se transmitieron. Está diseñado para conectar y enrutar, y tiene un grado muy elevado de fiabilidad, es adecuado para redes grandes y medianas, así como en redes empresariales. Puede detectar pérdida de información y errores de comunicaciones, disparando pedidos de retransmisión hasta que la información haya sido recibida completamente. Es uno de los protocolos fundamentales en Internet.

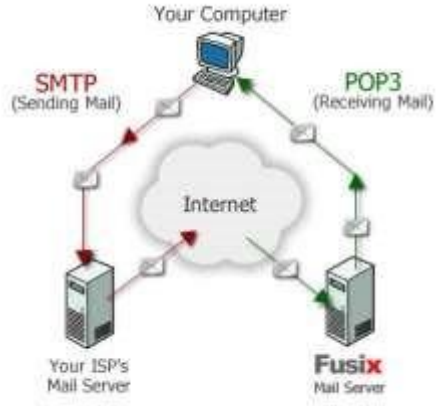
Muchos programas dentro de una red de datos compuesta por computadoras pueden usar TCP para crear *conexiones* entre ellos a través de las cuales puede enviarse un flujo de datos. El protocolo también proporciona un mecanismo para distinguir distintas aplicaciones dentro de una misma máquina, a través del concepto de puerto.

**TCP da soporte a muchas de las aplicaciones más populares de Internet** (navegadores, intercambio de ficheros, clientes ftp) y protocolos de aplicación HTTP, SMTP, SSH y FTP.

## PROTOCOLOS DE APLICACIÓN:


**HTTP:** Es el protocolo utilizado para identificar una URL, una página de internet. Es un protocolo sin estado, es decir, que no guarda ninguna información sobre conexiones anteriores. El desarrollo de aplicaciones web necesita frecuentemente mantener estado. Para esto se usan las **cookies**, que es información que un servidor puede almacenar en el sistema cliente. Esto le permite a las aplicaciones web instituir la noción de "sesión", y también permite rastrear usuarios ya que las cookies pueden guardarse en el cliente por tiempo indeterminado.

**SMTP:** Es el protocolo para el intercambio de información para transporte de mails.




**SSH:** Secure Shell, es utilizado para conexiones seguras, todo el tráfico que pasa por este protocolo lleva algún tipo de encriptación que lo hace ilegible para aquel que no sea el emisor o destinatario del mensaje.


**FTP:** Es un protocolo simple de transferencia de archivos, una página url que se identifica como ftp no presentara una gran información visual, en su generalidad presentara solo los archivos que el usuario creador desea compartir. Con el fin de facilitar la creación de una web, los servidores comerciales disponen de un sistema de FTP mediante el que se puede enviar rápidamente y de una sola vez todos los archivos que desees publicar en tu página u otros archivos: imágenes, audio, etc. Filezilla

***Concepto de Puerto****: El puerto es una numeración lógica que se asigna a las conexiones, tanto en el origen como en el destino. No tiene ninguna significación física.*

*El permitir o denegar acceso a los puertos es importante porque las aplicaciones servidoras (que aceptan conexiones originadas en otro ordenador) deben 'escuchar' en un puerto conocido de antemano para que un cliente (que inicia la conexión) pueda conectarse. Esto quiere decir que cuando el sistema operativo recibe una petición a ese puerto, la pasa a la aplicación que escucha en él, si hay alguna, y a ninguna otra.*


*Los servicios más habituales tienen asignados los llamados puertos bien conocidos,* ***por ejemplo el 80 para web, el 21 para ftp, el 23 para telnet****, etc. Así pues, cuando usted pide una página web, su navegador realiza una conexión al puerto 80 del servidor web, y si este número de puerto no se supiera de antemano o estuviera bloqueado no podría recibir la página.*

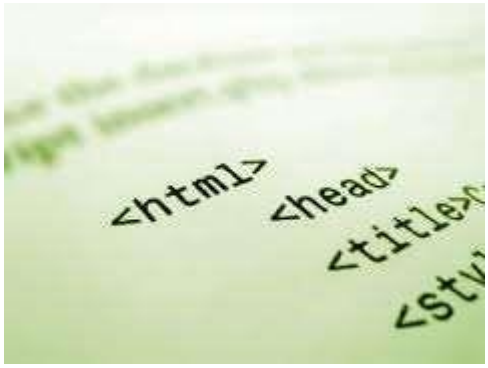
***Puerto abierto:*** *Acepta conexiones. Hay una aplicación escuchando en este puerto. Esto no quiere decir que se tenga acceso a la aplicación, sólo que hay posibilidad de conectarse.*

***Puerto Cerrado:*** *Se rechaza la conexión. Probablemente no hay aplicación escuchando en este puerto, o no se permite el acceso por alguna razón. Este es el comportamiento normal del sistema operativo.*

***Puerto bloqueado o Sigiloso:*** *No hay respuesta. Este es el estado ideal para un cliente en Internet, de esta forma ni siquiera se sabe si el ordenador está conectado. Normalmente este comportamiento se debe a un Firewall (Ver definición de firewall en "hardware de red") de algún tipo, o a que el ordenador está apagado.*

# Lenguajes


**HTML:** (HyperText Markup Language). Es un modo de codificar información sobre el contenido y la apariencia de una página web de modo de ser interpretada por el protocolo HTTP que es el que permite el intercambio de información en la Web.





**XML:** (E**x**tensible **M**arkup **L**anguage). Fue desarrollado World Wide Web Consortium (W3C) como un estándar para el intercambio de información estructurada entre diferentes plataformas, no solo Internet. Se puede usar en bases de datos, editores de texto, hojas de cálculo y otro tipo de archivos.

# Direcciones

## NÚMERO IP:

Es una combinación de números que identifican, de manera lógica y jerárquica, a cualquier equipo directamente conectado a Internet.


Los equipos que requieren de una conexión permanente a la red, como los servidores web o de correo, o los equipos empleados para transmisión de voz y imagen deben tener asignado un número de **IP fijo**, es decir invariable con el tiempo.

En cambio, las computadoras con acceso esporádico a la red. Empleadas para navegar, cuentan en general con un número de **IP variable**. Este tipo de metodología de asignación se logra con el

protocolo **DHCP** (Dynamic Host Configuration Protocol), que es un protocolo por el cual un router le asigna de manera automática y transparente para el usuario, un número de IP que cambia cada vez que se enciende el equipo. Este tipo de metodología es la más utilizada por los ISP que brindan servicios a hogares.

Existen Números de **IP internos**, que sirven para identificar una máquina dentro de una red local o LAN, y Números de **IP públicos**, que se emplean para navegar por internet o publicar archivos en la web como servidor.

Actualmente, en internet coexisten dos protocolos de direccionamiento:

**IPv4:** Es el protocolo "heredado". Su estructura de 32 bits permite aproximadamente 4.3 mil millones de direcciones (ej: 200.55.11.239). Este espacio numérico **se agotó oficialmente en 2011**, lo que significa que ya no se pueden asignar nuevos bloques de direcciones IPv4. Para extender su vida útil, se usan técnicas como NAT (Traducción de Direcciones de Red).

**IPv6:** Es el estándar actual y futuro de internet. Su arquitectura de 128 bits ofrece un número prácticamente ilimitado de direcciones (340 sextillones). Esto no solo soluciona el problema del agotamiento, sino que es **esencial para la expansión del Internet de las Cosas (IoT)**, redes 5G y la conexión de miles de millones de nuevos dispositivos. Un ejemplo de dirección IPv6 es 2001:0db8:85a3:0000:0000:8a2e:0370:7334.

**Transición y Estado Actual**: La transición de IPv4 a IPv6 no es un "apagón", sino una convivencia. La mayoría de las redes y sistemas operativos modernos operan en un modo llamado **"Doble Pila" (Dual Stack)**, donde son capaces de comunicarse usando tanto IPv4 como IPv6 simultáneamente, garantizando la compatibilidad. A nivel global y en Argentina, los principales proveedores de internet y de contenido ya han implementado IPv6 en sus redes troncales y ofrecen conectividad nativa a sus usuarios, aunque la adopción completa a nivel de usuario final sigue siendo un proceso gradual.

# DNS


Los números IP identifican cada equipo y permite una comunicación entre computadoras. El problema es que esa cantidad y combinación de números son difíciles de memorizar para los seres humanos, por eso se emplea en internet el servicio de **DNS** (Domain Name System).

Su función más importante, es traducir (resolver) nombres inteligibles para los humanos en identificadores binarios asociados con los equipos conectados a la red, esto con el propósito de poder localizar y direccionar estos equipos mundialmente.

El servidor DNS utiliza una base de datos distribuida y jerárquica que almacena información asociada a nombres de dominio en redes como Internet. Aunque como base de datos el DNS es capaz de asociar diferentes tipos de información a cada nombre, los usos más comunes son la asignación de nombres de dominio a direcciones IP y la localización de los servidores de correo electrónico de cada dominio.

La asignación de nombres a direcciones IP es ciertamente la función más conocida de los protocolos DNS. Por ejemplo, si la dirección IP del sitio FTP de prox.mx es 200.64.128.4, la mayoría de la gente llega a este equipo escribiendo en su navegador “ftp.prox.mx” y no la dirección IP. Además de ser más fácil de recordar, el nombre es más fiable ya que la dirección numérica podría cambiar por muchas razones, sin que tenga que cambiar el nombre.

Inicialmente, el DNS nació de la necesidad de recordar fácilmente los nombres de todos los servidores conectados a Internet.

**EJEMPLO PRÁCTICO:** Nosotros, como usuarios de internet, realizamos múltiples consultas a los DNS sin darnos cuenta. Tomemos como ejemplo que la dirección IP de la página www.google.com es 209.85.195.104.

Cuando escribimos en nuestro navegador www.google.com y presionamos la tecla “enter” nuestro navegador no consulta a internet por la pagina www.google.com sino que debe consultar por una dirección IP específica, entonces este debe primero obtener de alguna forma la dirección IP de esta

página, para esto realiza una primera verificación automática del cache de nuestra PC, si hemos accedido a esta página en un periodo de tiempo relativamente corto, los datos necesarios para acceder a esta página los tomara del cache, el cache es un archivo que mantiene un registro de los últimos sitios visitados y los datos específicos de los mismos, en el caso de nunca haber accedido a la misma se dispara una consulta al servidor DNS que tengamos configurado en nuestra PC, este Servidor DNS se puede cargar manualmente o, como en la mayoría de los casos, las PCs tienen una configuración dinámica que cuando encendemos nuestra PC, ella se encarga, a través del protocolo DHCP, de tomar una dirección IP para si misma y cargar los DNS automáticamente. Volviendo a la consulta, digamos que podemos ejemplificarla con 6 pasos.

1. Escribimos en el navegador www.google.com y presionamos la tecla “enter”.
2. Nuestra PC consulta a un servidor de DNS por la dirección IP de la página www.google.com.
3. El DNS resuelve la consulta y devolverá a la PC la dirección IP 209.85.195.104.
4. El navegador toma la IP y agrega el puerto 80, especificando que desea accede a contenido HTTP.
5. Envía a internet la instrucción por la dirección IP 209.85.195.104:80. (los : identifican al puerto)
6. El servidor descarga en nuestra PC el contenido de la página www.google.com.


**URL:** El URL es la cadena de caracteres con la cual se asigna una dirección única a cada uno de los recursos de información disponibles en la Internet. Existe un URL único para cada página de cada uno de los documentos de la World Wide Web. Un URL se clasifica por su esquema, que generalmente indica el protocolo de red que se usa para recuperar, a través de la red, la información del recurso identificado. Un URL comienza con el nombre de su esquema, seguido por dos puntos, seguido por una parte específica del esquema'

- *esquema://máquina/directorio/archivo*

También pueden añadirse otros datos:

- *esquema://usuario:contraseña@máquina:puerto/directorio/archivo*
- Por ejemplo: *http://ar.google.com/*

**URL en el uso diario:** Un HTTP URL combina en una dirección simple los elementos básicos de información necesarios para recuperar un recurso desde cualquier parte en la Internet:

1. El protocolo que se usa para comunicar,
2. El anfitrión (servidor) con el que se comunica,

   Un URL típico puede lucir como: http://ar.google.com