# CONCEPTOS BÁSICOS DE INTERNET

**Internet** no es una red sino un **conjunto de redes**. Este conjunto de redes permite la conexión de ordenadores y equipos a nivel global. Hoy en día prácticamente todas las redes utilizadas se conectan a internet o utilizan la misma tecnología que internet. ¿Por qué internet se ha convertido en la **mayor y única** red pública en el mundo? La respuesta más sencilla es que todas las tecnologías de red que se han desarrollado se pensaron para ser pequeñas. Internet nació grande y se pensó para ser grande. Aunque han sido necesarios algunos avances tecnológicos en estos años, ninguna tecnología ha conseguido llegar a ser tan grande como internet. Una vez convertido en un estándar ninguna tecnología de red ha podido competir con ella.

**Ethernet** es el medio más habitual por el que se comunican los datos hoy en día. Hablamos de conectores, tensiones, velocidades, etcétera. Sobre Ethernet se podría utilizar cualquier protocolo, aunque habitualmente se utiliza **TCP/IP**.

Una red ethernet se reconoce por los conectores, estos son como los del teléfono, pero a gran escala. El conector se denomina **RJ45** a diferencia del conector telefónico que se denomina RJ11. Los cables utilizados se denominan de «categoría 6».

Las velocidades que se alcanzan son de 100 Mbit/S y de 1000 Mbit/S (1 GBit/S). A nivel profesional existen redes ethernet de 10 GBit/S, pero la conexión se realiza mediante fibras ópticas con varios formatos en uso.

**Hub**. Antiguamente se utilizaba como base para una red ethernet. Todos los ordenadores se conectaban a un hub y en él se creaba la red ethernet. La red ethernet se denomina **de contienda**, es decir, aquí todos los ordenadores oyen a todos. Cuando un ordenador quiere mandar datos a otros, espera a que la red esté inactiva. En ese momento manda los mensajes y todos lo oyen. Solo el ordenador destino recibe el mensaje, los demás lo ignoran. Puede darse el caso de que dos ordenadores comiencen a mandar mensajes a la vez. En ese caso se dice que se ha producido una **colisión**, los dos se callan e intentan mandar el mensaje un poco más tarde. El hub es el encargado de que todos oigan a todos. Pueden conectarse dos hubs entre si y formarían parte de la misma red. Cuando hay muchos hubs

conectados entre si es necesario tener cuidado para no hacer bucles. Este equipo está en desuso, actualmente se utiliza el **switch**.

**MAC address** es la **dirección** utilizada en las redes ethernet. Cada equipo tiene una dirección MAC (Media Access Control) que se graba en fábrica. Si un ordenador tiene varios conectores de red tiene una dirección MAC por cada conector. Todos los mensajes que se emiten en una red internet llevan la dirección MAC de origen y la dirección MAC de destino. Solo hay una excepción: los mensajes denominados de «broadcast», estos solo tienen dirección MAC de origen y van destinados a todos los ordenadores conectados en la red.

**Switch** es la evolución del hub y permite que haya varias conexiones simultáneas, minimizando las colisiones. El switch apunta la dirección MAC de cada ordenador conectado. Cuando un ordenador envía un mensaje a otro el switch mira a quien va destinado y solo manda el mensaje por el conector donde está conectado el ordenador destino. Como los demás se piensan que la red está inactiva siguen mandando mensajes. El switch se encarga de que los mensajes lleguen a su destino y los demás ordenadores piensen que la red está inactiva. De esta manera se pueden dar muchas comunicaciones simultáneas y aumenta muchísimo la capacidad de la red. Solo los mensajes de broadcast se envían a todos los conectores, aunque normalmente son muy pocos. Al igual que el hub se pueden conectar varios switches entre si para prevenir los bucles y utilizar solo un cable para esa conexión.

El **Protocolo** describe los procedimientos para enviar datos a través de un medio. Imaginemos el correo de toda la vida. El medio serían los sobres, los carteros, camiones, sacos de correo, etcétera. El protocolo indicaría que debemos meter los datos en un sobre, escribir la dirección de destino en el frontal del sobre, poner el sello adecuado para la distancia y la dirección remitente en la parte de atrás del sobre. Los protocolos también se podrían anidar, imaginemos que enviamos una carta a una persona de una gran empresa, la carta llegaría a la sede principal y, en ella, la persona encargada del correo introduciría dicha carta en un sobre de correo interno con el que la carta llegaría finalmente al destinatario.

En el mundo informático el protocolo más importante hoy en día es el protocolo **TCP/IP** y, en internet, es sobre el que pivotan todas las comunicaciones, pero no es el único. Existen varios protocolos complementarios a TCP/IP y multitud de protocolos que utilizan TCP/IP como

base. Por ejemplo, **HTTP** es el protocolo básico para el servicio WEB y es el utilizado por todos los navegadores. HTTP es un protocolo que funciona sobre TCP/IP. Para el análisis de los protocolos utilizados en internet existe una herramienta muy potente (y gratuita) llamada Wireshark con la que podemos observar, analizar y comprender los protocolos utilizados en la comunicación de nuestro ordenador.

**TCP/IP** es el protocolo más utilizado hoy en día y prácticamente se ha convertido en el protocolo único. Explicar TCP/IP se basa en que todos los ordenadores y equipos tiene una dirección llamada dirección IP. Cada dirección IP son cuatro números de 0 a 255. Un ejemplo de dirección IP sería 156.132.45.67. Todo paquete de datos llevaría la dirección de origen y la dirección de destino. La red se encarga de que el paquete llegue a su destino.

**ARP** es el protocolo que se utiliza antes de una comunicación TCP/IP. Cuando un ordenador quiere mandar un mensaje a una dirección IP debe saber primero su dirección MAC ya que esta es la única que vale en una red ethernet. Mediante el protocolo ARP se manda un mensaje de broadcast a todos los ordenadores preguntando quien tiene esa dirección IP. Solo el ordenador indicado responde indicando su dirección MAC. Los ordenadores guardan una relación entre dirección IP y dirección MAC y solo utilizan el protocolo ARP la primera vez o cuando algo falla.

El **Router** es el equipo que conecta dos redes distintas que pueden incluso ser de tecnologías diferentes. Funciona solo a nivel de protocolo TCP/IP y envía de una red a otra solo los mensajes que van de una red a otra. Realmente el router no analiza los mensajes que se mandan por cada red. Cada ordenador sabe perfectamente cuando el mensaje va a otro ordenador de la misma red y cuando va a otro ordenador de otra red. La configuración que determina esto es la máscara que es parte de la configuración. También, cuando se configura un ordenador se indica la dirección IP del router por lo que, cuando el destinatario no está en la red, se envía el mensaje al router (en la configuración se denomina gateway) y el router se encarga de mandarlo por la red adecuada.

La **Máscara** discrimina cuando el ordenador destino está en la misma red o está en otra red. La más habitual es «255.255.255.0». Cualquier otra máscara es para expertos.

La dirección IP es un conjunto de 4 números de 0 a 255. Esta máscara indica que los tres primeros números corresponden a la red y el último al ordenador. Si nuestro ordenador tiene la dirección 192.168.1.45 y el mensaje va al ordenador 192.168.1.78, estarían en la misma red. Si la dirección destino es 192.168.4.32 estarían en redes distintas, entonces el mensaje se mandaría a la dirección del router que normalmente sería la 192.168.1.1.

El **Protocolo DHCP** es complementario de TCP/IP y es utilizado esporádicamente. Sirve para asignar a un ordenador que se enciende la configuración TCP/IP necesaria para poder comunicarse. Normalmente el router ADSL que tenemos en nuestra casa es, a su vez, servidor DHCP asignando la configuración adecuada a cada ordenador o equipo. La configuración básica para poder conectarse es la siguiente: dirección IP, máscara, dirección IP del router (gateway), dirección o direcciones de los servidores DNS. Esta configuración, cuando indicamos configuración automática, es recibida del servidor DHCP.

El **sistema DNS** (Domain Name Server) se encarga de traducir la dirección IP a "texto", pues sería complicado tener que acordarnos de que la página web de un periódico es la dirección 156.132.45.67, Es mucho más fácil acordarse de www.periodico.com. Cuando introducimos www.periodico.com el ordenador automáticamente se conecta al DNS y este le devuelve la dirección (el juego de 4 números) necesario para comunicarse. Todos los proveedores de internet tienen un servidor DNS para sus usuarios. Cuando este DNS no tiene la traducción consulta a otro DNS de rango superior.

**NAT** (Network Address Translator) o traducción de direcciones en la red, es una función muy utilizada sobre todo cuando queremos adaptar una red privada a una red pública. Por ejemplo, cuando conectamos un ordenador al router de nuestra casa nos da una dirección que empieza por 192.168.X.X. La inmensa mayoría de las redes domésticas asignan direcciones que empiezan por 192.168. Esto es así porque este rango de direcciones no existe en Internet y está reservado para redes privadas como la de nuestra casa. Si tenemos varios ordenadores todos comparten los tres primeros números y solo cambia el último. Por ejemplo 192.168.1.30, 192.168.1.31 y 192.168.1.32; estas direcciones no son validas en Internet. Los paquetes de datos en Internet llevan la dirección IP a la que van destinados y la dirección IP de la que parten. Al pasar por el router es necesario cambiar la dirección origen por una válida en Internet. ¿Por cual? Cada router conectado a internet tiene asignada una única dirección IP

válida en Internet. Todos los paquetes de datos que salen hacia internet cambian su dirección origen por la dirección del router ¿Y qué ocurre a la vuelta con los paquetes que vienen de internet? El router sabe cuando un paquete es contestación de uno que mandó y hace el cambio opuesto mandándolo al ordenador adecuado. ¿Y qué ocurre con los paquetes que vienen de internet que no son contestación de ninguno que se mandó? Sencillamente se pierden. Este es su mecanismo de seguridad ya que cualquier ataque que recibamos no pasará del router porque no es contestación de ningún paquete que nosotros hemos enviado. Los rangos asignados para redes privadas son: 10.X.X.X, del 172.16.X.X al 172.31.X.X, el 169.254.X.X y el 192.168.X.X. Cualquier dirección que esté en estos rangos es una dirección de una red privada y necesitará la función NAT del router para conectarse a internet. Los rangos son bastante amplios para permitir redes privadas incluso para grandes empresas.

***Referencia:***

*Temas Tecnológicos de Interés (s.f.) Conceptos básicos de Internet. ¿Qué necesito saber? Recuperado de: https://www.temastecnologicos.com/internet/*