Clase 13: Protocolos de internet.

¿Cómo funciona el internet?

El protocolo de Internet o IP —Internet Protocol—, es el protocolo principal y su importancia es fundamental para el intercambio de mensajes en redes informáticas, ya que establece las normas para dicho intercambio.

Este, junto al protocolo de control de transmisiones —TCP o Transmission Control Protocol—, sientan las bases de Internet y permiten la comunicación entre los dispositivos o computadoras pertenecientes a una red sin importar si el software o el hardware de cada uno es diferente. Para que el remitente pueda enviar un paquete de datos al destinatario, el protocolo IP define una estructura de paquetes que agrupa los datos que se tienen que enviar. En la cabecera de dicho paquete irá la información sobre el origen y el destino de los datos.

Protocolo de internet IP.

IP —Internet Protocol, en inglés— es un protocolo de comunicación de datos digitales clasificado funcionalmente en la capa de red —que es la que nos proporciona conectividad y la selección de ruta entre dos sistemas hosts—. La función principal es conseguir que los datos lleguen desde origen al destino, aunque no tenga una conexión directa. Estos datos se transfieren mediante paquetes conmutados —método de agrupar los datos transmitidos a través de una red digital en paquetes, estos están compuestos por los datos en sí y la información de control que nos indicará cual es la ruta que debe tomar para que los datos lleguen a destino—.

Este protocolo se encargará de buscar el mejor método de enrutamiento, sin garantías de alcanzar el destino final, pero aun así trata de buscar la mejor ruta entre las conocidas por la máquina que esté usando IP.

Protocolo de control de Transmisión TCP.

El TCP —Transmission Control Protocol, en inglés— garantiza que los datos sean entregados al lugar de destino, sin ningún error y en el mismo orden que se transmitieron. Se encuentra en una capa intermedia entre el protocolo IP y la aplicación y, esta ubicación se debe a que la aplicación necesita que la comunicación de la red sea confiable. El protocolo TCP

da soporte a muchas de las aplicaciones más populares de Internet

—navegadores, intercambio de ficheros, etcétera— y protocolos de aplicación HTTP, SSH, FTP, entre otros.

Protocolo DNS.

El sistema de nombres de dominio —DNS, en inglés Domain Name System—, es un sistema de nomenclatura jerárquico descentralizado para dispositivos conectados tanto a Internet como a redes privadas, que asocia información con el nombre del dominio. Su función principal es “traducir” los nombres de los dominios que estamos acostumbrados, como youtube.com, en identificadores binarios asociados con los equipos conectados a la red o direcciones IP, como 84.78.754.20.

Para acceder a Internet los usuarios utilizan el nombre de dominio, en lugar de los complejos números de IP. Para ello, Internet utiliza su “agenda grande ” llamada DNS. El servidor DNS proporciona este servicio a Internet.

Protocolo TCP/IP.

El TCP/IP —protocolo de control de transmisión/protocolo de Internet— consiste en una combinación de los protocolos previamente mencionados y son la piedra angular de las redes informáticas modernas.

Es usado para comunicaciones en redes y, como todo protocolo, describe un conjunto de guías generales de operación para permitir que un equipo pueda comunicarse en una red. TCP/IP provee conectividad de extremo a extremo especificando cómo los datos deberían ser formateados, direccionados, transmitidos, enrutados y recibidos por el destinatario.

Protocolo UDP.

El protocolo de datagramas de usuario —UDP, en inglés User Datagram Protocol— es un protocolo del nivel de transporte basado en el intercambio de datagramas —un datagrama es un paquete de datos, es cada uno de los bloques en que se divide la información para enviar—.

Su función es permitir el envío de datagramas a través de la red sin que se haya establecido previamente una conexión ya que el propio datagrama incorpora suficiente información de direccionamiento en su cabecera.

El protocolo UDP es más ligero ya que no utiliza tantas capas como el protocolo TCP/IP porque no existe un control sobre el envío de los paquetes.

Al ser orientada a la no conexión lo único que le interesa a este protocolo es enviar los datagramas lo más rápido posible, sin tener en cuenta si el paquete llegó completo o no. Se utiliza comúnmente para la transmisión de datos de alta velocidad, por ejemplo para streaming, juegos online, entre otros.

Protocolo HTTP.

El protocolo de transferencia de hipertexto —HTTP, en inglés Hypertext Transfer Protocol— es un protocolo orientado a transacciones y sigue el esquema petición-respuesta entre un cliente y un servidor. El cliente —normalmente un navegador web— realiza una petición enviando un mensaje, con cierto formato al servidor. El servidor —o servidor web— le envía un mensaje de respuesta, permitiendo la comunicación entre ambos. No está protegida y podríamos pensar que toda la información está en texto puro. Si alguien intercepta una comunicación, podría ver nuestros datos.

Protocolo HTTPS.

El protocolo seguro de transferencia de hipertexto —en inglés, Hypertext Transfer Protocol Secure o HTTPS— está destinado a la transferencia segura de datos de hipertexto. Lo que hace es encriptar los datos que son enviados entre clientes y servidores utilizando algoritmos, de este modo toda la información sensible, como números de tarjetas, pueden ser enviados de manera segura. Si alguien intercepta una comunicación obtendría un mensaje encriptado y este va a ser muy difícil de desencriptar.

Dirección IP.

Según el protocolo IP, cada equipo tiene una dirección IP numérica única que lo ubica en la red a la que está conectado.

Una dirección IP es una cadena de números separados por puntos. Cada conjunto de números se denomina octeto.

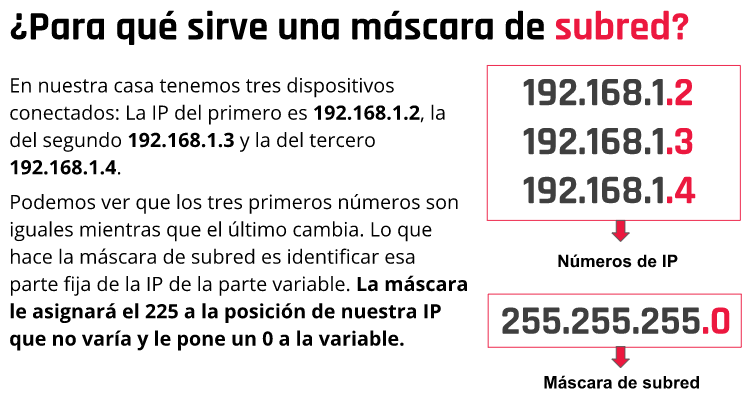


Cada octeto puede contener números que van del 0 al 255. Cada octeto está formado por 8 bits, 255 es el número más grande que puede ser formado por un número de 8 bits. Cada dirección está compuesta por un número de red y un número de host. La porción del número que identifica a la red varía en base a las clases.

* Clase A: Número de red de un solo octeto y el resto numero de host. (compañías internacionales)
* Clase B: Dos octetos de host. (universidades)
* Clase C: Un octeto de host. (redes de casas)

Este sistema se denomina IPv4 y ya se encuentra saturado (es de los 90) por lo que se desarrolló uno nuevo, el IPv6, aunque el IPv4 sigue siendo el más usado. Un sistema que se utiliza actualmente para evitar la saturación en el IPv4 es la utilización de IP privadas, ya que estas no requieren que sean únicas como las públicas, sólo deben ser distintas a las otras direcciones IP que se encuentren en la misma red. La IP privada de un dispositivo es diferente a su IP pública.

SubRed.



Direcciones IP importantes.

|  |  |
| --- | --- |
| **Nombre** | Descripción |
| **Router** | La primera dirección disponible (por ejemplo 192.168.1.1) corresponde al router, el dispositivo que hace enlace con las otras redes, como Internet. De este modo, todos los dispositivos que quieran consultar algo en Internet lo primero que deben hacer es enviar la petición a la dirección del router, el cual se encargará de redirigir la petición. |
| **Broadcast** | Es la dirección más alta de la red a la que pertenezca el dispositivo, y es utilizada por el router para enviar un mensaje de difusión a todos los dispositivos que tengan una IP asignada dentro de la red, en redes hogareñas generalmente es 192.168.1.255 |

IPv6.

IPv6 es la versión 6 del protocolo de Internet. Está destinada a sustituir al estándar IPv4 ya que la anterior versión cuenta con un límite de direcciones de red que impide el crecimiento de la misma.

|  |  |
| --- | --- |
| **Ventajas** | Descripción |
| **Número casi ilimitado de IPs únicas** | Este nuevo protocolo permite que cada dispositivo conectado a Internet tenga su propia dirección IP. Una ventaja que poco a poco se va convirtiendo en un requisito con el continuo avance del Internet de las cosas. |
| **Autoconfiguración** | El nuevo protocolo consta de mejores métodos para realizar la configuración automática, lo que supone una mejora significativa respecto al clásico DHCP utilizado en IPv4. |
| **Más seguridad** | El protocolo IPv6 puede ser mejorado con IPsec (Internet Protocol Security, en inglés) para gestionar la encriptación y autenticación entre hosts. Proporciona un sólido marco de seguridad de punto a punto en la transferencia de datos. |
| **Más eficiencia** | La gestión de paquetes es mucho más eficiente en IPv6. |

Actividad.

