Clase 14

Redes internas

Enrutamiento y puertos:

**Routing**: acción de mover datos de una red a otra. Lo lleva a cabo el **router**

**Router**: es quien permite interconectar computadoras estableciendo qué rutas seguirán mis datos.

Realiza las siguientes acciones:

1. Recibe el paquete de datos
2. Busca cuál es la dirección de destino
3. Verifica la tabla de enrutamiento que tiene configurada
4. Procede a enviar el paquete a destino por la mejor ruta posible

Para recibir o enviar información, el router utiliza **tablas de enrutamiento**, que son un conjunto de reglas que sirven para determinar qué camino deben seguir los paquetes de datos.

Las **tablas de enrutamiento** contienen toda la información necesaria para hacer que uno o varios paquetes de datos puedan viajar a través de la red usando el mejor camino. Estas, se componen, entre otros componentes, de:

* **Red de destino:** corresponde a la red de destino donde deberá ir el paquete de datos.
* **Siguiente salto:** es la dirección IP de la interfaz de red por donde viajará el paquete de datos para seguir con su camino hasta el final.
* **Interfaz de salida:** es la interfaz de red por donde deben salir los paquetes para llegar posteriormente a destino.

**Tipos de enrutamiento:**

* **Enrutamiento estático:** las tablas se crean de forma manual. El administrador de redes las configura con la información de cómo alcanzar las diferentes redes remotas. Este es responsable de que las redes sean accesibles y estén libres de bugs e inconsistencias.
  + Consume menos anchoo de banda
  + Consume menos memoria
  + Se utiliza para redes pequeñas
  + No es escalable

**Ventajas:** aunque el mantenimiento es complicado, no se consume ancho de banda de red para enviar mensajes entre routers.

**Desventajas:** cualquier cambio en la red requiere que el administrador agregue o elimine las rutas afectadas por dichos cambios.

* **Enrutamiento dinámico:** la información necesaria para crear y mantener actualizadas las tablas se obtienen de los demás routers de la red. Estos utilizan protocolos de enrutamiento para intercambiar información con sus routers vecinos.
  + Alto consumo de ancho de banda
  + Alto consumo de memoria
  + Se utiliza para redes grandes
  + Es automático

**Ventajas:** el administrador solo pone en marcha el enrutamiento dinámico, luego las tablas de enrutamiento se ajustan automáticamente ante cambios en la red.

**Desventajas:** consumo mucho ancho de banda, debido a los mensajes que se intercambian los routers para configurarse automáticamente.

**Puertos:** son puntos de conexión para el intercambio de información y la transmisión de datos.

Cuando enviamos datos desde nuestra red local a la externa el router utiliza una serie de canales o puertas en las que se organiza el contenido que enviamos. Estos son los **puertos**. Funcionan como puertas que se abren y cierran y permiten el paso de la información que enviamos o recibimos en la red.’

Todos los routers tienen un total de 65536 puertos que van desde el 0 al 65535. La IANA, entidad que supervisa la asignación global de direcciones IP y otros recursos relativos a los protocolos de internet tienen establecido un estándar de asignación de puertos.

**Existen 3 grupos de puertos que tienen una función específica:**

* **Puertos del 0 al 1023:** son los que están reservados para el sistema operativo de la computadora y los protocolos más importantes para su funcionamiento
* **Puertos del 1024 al 49151:** son los puertos registrados, los que se utilizan por las aplicaciones y los juegos que instales en la computadora.
* **Puertos del 49152 al 65535:** puertos dinámicos o privados, corresponden a las aplicaciones que necesitan conectarse a un servidor.

**Redes de direccionamiento externo:**

Cuando nuestros datos salen del router viajan fuera de nuestra red local y van directamente a parar al **ISP *(Proveedor de Servicios de Internet)***, que es la empresa que nos brinda conexión a internet a través de diferentes tecnologías como Fibra óptica, Banda ancha, Cable modem, 3g, 4g, entre otros servicios.

Antes del 2018 la mayoría del tráfico no viajaba encriptado, pero en la actualidad la mayoría de nuestros paquetes de datos viajan protegidos y solo es visible a dónde viaja pero no el contenido.

Los **ISP** reciben todos lo paquetes de datos que enviamos y los envían a su destino, pudiendo aplicar filtros de normativas referentes a bloquear páginas de piratería, contenido protegido geográficamente o políticas gubernamentales según lo que determine cada gobierno.

En internet existen distintos protocolos que hacen esto que llamamos **direccionamiento externo** uno es el **Proxy** equipo informático que intercepta conexiones de red hechas desde un cliente a un servidor de destino **eludiendo** así **al** **ISP**.

Otro método es una **VPN (red privada virtual)** tecnología que permite una extensión segura de una red local sobre una red pública como Internet, permite que nuestra computadora envíe y reciba dato conectándose a otras redes compartidas o publicas como si fueran una red privada con toda la funcionalidad, seguridad, y políticas de gestión de una red privada.

**VPN:** o ***red privada virtual***, es una tecnología que protege nuestra privacidad cuando utilizamos Internet dirigiendo nuestra conexión a través de un servidor que oculta la dirección IP y encripta la comunicación online.

Cuando se utiliza una VPN, la información enviada desde la computadora pasa a través de uno de los servidores del proveedor de VPN antes de llegar a su destino.

**Ventajas:**

* Son fáciles de instalar y utilizar
* La velocidad no se ve afectada por el software de cifrado y los servidores
* Compatibilidad con la mayoría de los dispositivos

**Desventajas:**

* Encriptación débil
* Fallos del software, que pueden ocasionar que los mensajes viajen sin cifrar y fuera de la red VPN
* Políticas de registro variadas

**TOR:** red de anonimato que se encuentra distribuida y superpuesta sobre Internet en la que el direccionamiento de los mensajes intercambiados entre los usuarios no revela su dirección IP, además mantiene la integridad y el secreto de la información que viaja por ella.

A primera vista, es similar a una VPN. Pero donde las VPN brindan privacidad, Tor brinda **anonimato.**

**Ventajas:**

* Difíciles de apagar. La red está distribuida por lo que no hay un lugar central para hacerlo.
* Anonimato completo

**Desventajas:**

* Lentitud: los mensajes pasan por tres o más servidores y se cifran y descifran al menos 3 veces
* Dirigida por voluntarios: por lo tanto, no hay ingresos para actualizaciones y mantenimiento
* Baja compatibilidad con dispositivos