CLASE ANTERIOR:

URL: Direcciones web. (Nombre: Lucas) Está compuesta por lo que es el protocolo y el dominio a donde vamos a entrar. <http://www.lagaceta.com.ar>. Hoy utilizamos más que nada URL.  
URI: Se compone de URL y el URN, puede ser una o la otra, o ambas. Lo que ponemos en un navegador para navegar. <http://www.lagaceta.com.ar/articulo1> Una dirección URI completa.  
URN: (Numero de documento: 37617130)[www.lagaceta.com.ar/articulo1](http://www.lagaceta.com.ar/articulo1) Dirección exacta del artículo que queremos entrar, entras sin protocolos directamente al recurso. (http://). Mucho más específica.

CLASE 14:

video

Direccionamiento interno:

¿Como se transmite la información que enviamos a través de internet para que llegue en segundos?  
Utilizando el routing (enrutamiento) que es la acción de mover datos de una red a otra.

¿Como funciona el routing?   
Lo lleva a cabo el router. Permite interconectar computadoras estableciendo que rutas seguirán mis datos. LA información viaja a través de cientos de miles de router hasta llegar a destino.   
Ejemplo: Mi computadora pertenece a esta red: 192.168.1.0 que tiene una dirección IP: 192.168.1.5  
Cuando queremos ingresar a una página web, (Google) nuestra computadora envía una solicitud a través del navegador. Primero traduce <http://www.google.com> en una dirección IP, esa será la dirección a la que viajará la solicitud de visualización de la página:  
Destino: 142.251.33.100  
Mensaje: Solicitud de visualización de una pagina web.  
Esa solicitud sale como un mensaje a mi router de mi red local. El router es quien nos comunicara con el exterior. Cuando el mensaje llega al router, este busca cual es la dirección de destino, reconoce que esa dirección no pertenece a nuestra red local y verifica en la tabla de enrutamiento que tiene configurada cual es la ruta posible para que el mensaje llegue a destino.  
En esa ruta habrá mas router que irán pasando el mensaje uno a uno, una vez que el mensaje llega a la computadora de destino esta responde con la información que satisface la solicitud: la pagina web. Esa información viaja nuevamente a través de los routers hasta llegar a mi computadora, a mi navegador para visualizarse.   
La conexión entre dos computadoras siempre se establece de la misma forma: a través de direcciones IP.   
¿Pero qué pasa si queremos obtener diferentes servicios de la otra computadora?  
Por ejemplo: Conectarnos a la pagina web y al servicio de mail que provee.

¿Como diferenciamos esas solicitudes si hay una sola conexión? Las diferenciamos a través de puertos. Cada dispositivo tiene miles de ellos, 65536. Cada uno destinado a enviar o recibir cierto tipo de información. Los mas conocidos van del 0 al 1023 y son los que están reservados para el sistema operativo y los protocolos de red más importantes.  
21: FTP  
25: SMTP   
80 HTTP  
1024-49151: aplicaciones y juegos  
49151 o +: puertos dinámicos o privados.  
Cuando solicitamos una pagina web hicimos una petición de tipo HTTP lo que significa que solicitaremos esa información al puerto 80 de la computadora que contiene la página. Esta información viaja junto a la dirección IP (142.251.33.100:80). Al mismo tiempo se genera un puerto aleatorio para mi computadora en el que recibirá la información de respuesta. Cuando el mensaje llega a la computadora de destino, esta sabe que debe responder a con una pagina web porque la petición ingreso por su puerto 80. Esa respuesta vuelve a nuestra PC por los routers, ingresa por el puerto aleatorio y la pagina web se puede visualizar. Tarda milisegundos.

¿Qué función tiene un router en la red?  
1. Recibe el paquete de datos  
2.Busca cual 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.

¿Como hace un router para enviar y recibir información?   
Un router, para recibir o enviar información, utiliza tablas de enrutamiento, que son un conjunto de reglas que sirven para determinar que 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 utilizando el mejor camino.

Componentes de una tabla de enrutamiento:  
\*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 viajara 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 red las configura con la información de como alcanzar las diferentes redes remotas. Este es responsable de que las redes sean accesibles y estén libres de bugs e inconsistencias:  
\*Consume menos ancho de la banca  
\*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 elimines 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  
Ventas: El administrador solo pone en marcha el enrutamiento dinámico, luego las tablas de enrutamiento se ajustan automáticamente ante cambios en la red.  
Desventajas: Consume 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 tiene 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 mas 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 EXTERNAS:

Redes de direccionamiento externo:   
Cuando nuestros datos salen del router viajan fuera de nuestra red local y van directamente a parar a 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 los paquetes de datos viajan protegidos y solo es visible a donde viaja, pero no el contenido. Los ISP reciben todos los datos que enviamos y los envían a su destino, pudiendo aplicar filtros de normativas referentes a bloquear páginas de piratería (robo de datos), contenido protegido geográficamente (Falsificación de mensajes) o políticas gubernamentales según lo que determine cada gobierno(espionaje). SSL???  
En internet existen distintos protocolos que hacen esto que llamamos direccionamiento externo.   
-Proxy: Se trata de un equipo informático que intercepta conexiones de red, hechas desde un cliente hacia un servidor de destino eludiendo así al ISP.  
-VPN o red privada virtual: Es una tecnología que permite una extensión segura de la red local sobre una red publica como internet. Permite que nuestra computadora envíe y reciba datos conectándose a otras redes compartidas o publicas como si fueran una red privada con todas las funcionalidad, seguridad y policitas de gestión de una red privada. Algunas empresas permiten acceso a algunos recursos de sus servidores locales a las personas que se encuentran en su misma red.   
-TOR: una red de anonimato que se encuentra distribuida y superpuesta sobre internet, en la que los direccionamientos en los mensajes intercambiados entre los usuarios no relevan su dirección IP, además mantiene la integridad y el secreto de la información que viaja por ella. Para esto, primero el usuario accede a un intermediario de la red TOR que sabe la identidad del usuario, pero no con quien se comunicara. Y el ultimo intermediario sabe con quién se comunica, pero no quien es el usuario que envía el mensaje.

VIDEO …  
PPT…

VPN:   
Una red privada virtual o por sus siglas en ingles también llamada VPN, 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  
-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: Esto puede ocasionar que los mensajes viajen sin cifrar y fuera de la red VPN.  
-Políticas de registro variadas

TOR:  
A primera vista, la red Tor es similar a una VPN. Los mensajes hacia y desde su computadora pasan a través de la red Tor en lugar de conectarse directamente a los recursos de Internet. Pero donde las VPN brindan privacidad, Tor brinda anonimato.  
Ventajas:   
-Difícil de apagar: La red esta distribuida por lo que no hay lugar central para hacerlo.  
-Anonimato casi completo  
Desventajas:  
-Lentitud: Los mensajes pasan por tres o mas 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.

![Imagen que contiene nombre de la empresa

Descripción generada automáticamente]()

PROTOCOLO NAT: va de cierta forma traduciendo entre todos los routers ¿?

PREGUNTAR COMO CAMBIIAR LA REGION DEL CELULAR?

A TRAVES DEL PUERTO DEFINE O LE DICE AL SERVIDOR QUE ES LO QUE QUIERE LA PERSONA PARA RESPONDERLE EN BASE A ESO.