# Introducción a la informática

## Módulo 4. Surfeando Internet

## Clase 16. Redes

## Julio 5 de 2021

Red Informática: Conjunto de dispositivos informáticos conectados entre sí, y que envían y reciben datos para compartir información y recursos.

**Funciones:**
- Confiabilidad
- Disponibilidad
- Aumentar la velocidad
- Reducir costos

**Clasificación de Redes:**

**Redes por alcance**

- PAN: Red de Area Personal. Conexión con los dispositivos.

- LAN: Red de área local. 1 a 5 km.

- MAN: Red de área metropolitana. Alrededor de 50 – 60 km.

- WAN: Red de area amplia. 100 – 1000 km.

Otras clasificaciónes: Nano / BAN / PAN / LAN / CAN / MAN / RAN / WAN

**Por Grado de autenticación**

- Privada

- De acceso público

**Por tipo de Conexión**

- Cableado. Utilizan componentes físicos y sólidos. Par trenzado / Cable Coaxial / Fibra Óptica

- Redes inalámbricas. Infrarrojo / Blootooth (10m) / WiFi (100m al aire libre).

**Por Grado de difusión**

- Intranet
- Extranet
- Internet. Es un conjunto descentralizado de redes de comunicación interconectadas que utilizan la familia de protocolos TCP/IP, garantizando que las redes físicas heterogéneas que la componen funcionen como una red lógica única, de alcance mundial.

## Medios de transmisión de la información

Medios guiados: Pares trenzados / Cable coaxial / Fibra óptica

Medios no guiados: Señales de Blootooth / Señales de Infrarrojo / Señales de WiFi

**Pares trenzados:**
Vmax = 1 Gbps
d = 2 – 10 km (distancia entre repetidores)

**Cable coaxial:**
Vmax = 2 Gbps
d = 10 – 100 km

**Fibra óptica:**
Vmax = 10 Gbps
d > 100 km

## Velocidades de Internet

Características de una red de datos:

- Velocidad
- Seguridad
- Confiabilidad
- Escalabilidad
- Disponibilidad

## Armar mi propia red en casa

- Listar los dispositivos.
- Identificar cuáles requieren conexión por cable y cuáles usan WiFi.
- Realizar un croquis
- Diseñar la red, ubicar el router estratégico. Se requiere router con modem integrado. El router separa la red pública de la red privada.
- Lanzar cable de red, tipo UTP categoría 5E o 6.
- En los extremos deben tener fichas RJ45.

## Componentes básicos de la red

Hub: Interconecta los ordenadores de la red local. Recibe señal de uno de los equipos y la replica a todos los demás.

Switch: Recibe señal de uno de los equipos y la envía directamente al destinatario.

Módem: Se encuentra entre el router y la línea de la operadora. Cuando se establece conexión con el operador, obtiene una dirección IP pública, que identifica la conexión.

Router: Se conecta al módem y a todos los dispositivos. Puede recibir información a transmitirla por cable o por WiFi. El router asigna una IP local a cada dispositivo, lleva Internet a cada uno de ellos y permite crear la LAN.

PLC vs Repetidor WiFi:

PLC: Mejor rendimiento, mayor cobertura, mayor estabilidad y mayor precio.

## Guía de Troubleshooting

Paso 1: chequear hardware.
Paso 2: Utilizar el comando "ipconfig". La puerta de enlace es la IP del router. La IP de la computadora aparece como "Dirección IP"
Paso 3: Utilizar los comando "ping" y "tracert". ping 8.8.8.8 verifica la posibilidad de enviar y recibir mensajes. Ping 8.8.8.8 -t repete la operación indefinidamente.
Paso 4: Utilizar el comando "nslookup". Determina si hay un problema con el servidor al cual se está tratando de acceder. Ej: nslookup es.wikipedia.org.

## Sincrónico

## Medios de transmisión

El par trenzado ha reemplazado al cable coaxial por su mayor capacidad de transmisión de datos, y porque es mucho más barato que la fibra óptica.

Trenzar el cable ayuda a evitar la interferencia por el magnetismo.

Todos los tipos de cables (excepto la fibra óptica) tienen una limitación en la longitud máxima en la que pueden transmitir la información de forma segura, debido a la resistencia del componente.

Cable coaxial: Hasta 150m  sin pérdida

Cable UTP: Hasta 100m sin pérdida, aunque se puede extender con repetidores.

Rack: Caja donde se pueden conectar switches, servidores, etc.

Pachera: Organizador de las conexiones.

Cables trenzados:
UT
STP
SFTP: actual
Se diferencia en la capacidad de transmisión. (10M, 1G, 50G aproximadamente, respectivamente).

Dos formas de comunicación en Internet: sincrónica y asincrónica.

En los hogares se usa conexión asincrónica, debido a que utilizamos Internet principalmente para bajar información.

Los grandes servidores utilizan conexión sincrónica (o simétrica), donde las velocidades de subida y de bajada son iguales.

Test de velocidad:
- Ping Ideal de 1 a 13
- Aceptable hasta 50
- Alto por encima de 50.

Lo que viene:
- LiFi
- 6G

**Componentes de Red**

- Hub: Dispositivo antiguo e ineficiente. Genera choques de paquetes. El hub hace un envío masivo a todos los componentes (broadcast). El hub no discrimina la información.
Actualmente los hub no se utilizan en redes, aunque sí se utilizan, por ejemplo, en los dispositivos que amplían las ranuras USB

- Switch: Dispositivo Capa 2.

- Router: Similar al switch, pero en vez de conectar computadoras, conecta redes. Se conecta con otras redes; es un dispositivo de capa 3.

- Modem: Modula las señales. El modem convierte las señales analógicas en señales digitales, para que la computadora pueda entenderlo. Algunos modems pueden también funcionar como routers.

Tecnologías modernas no necesitan modem (Ej Gpon), ya que hacen una distribución amplia en señales electromagnéticas.

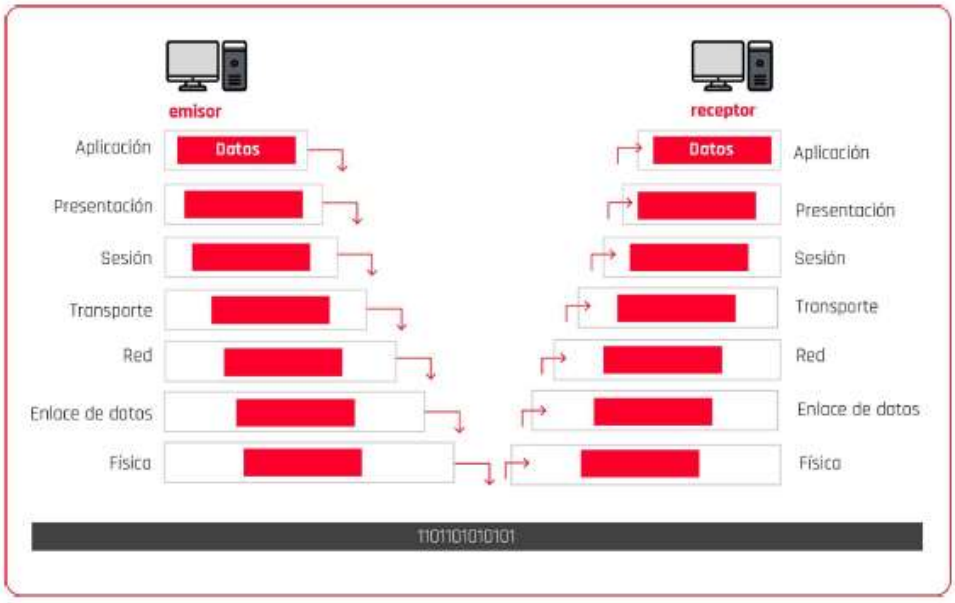
El switch trabaja con direcciones físicas (Mac), mientras que el router trabaja con direcciones IP.

**Velocidades de Internet**

## Clase 17. Protocolos de Internet (inicial) I

### ¿Qué es el modelo OSI?

Es un modelo conceptual de interconexión que permite que diversos sistemas se comuniquen mediante un estándar. Se basa en la idea de dividir un sistema de comunicación en 7 capas y cada una de ellas trabaja sobre la precedente.




La capa de transporte segmenta los datos y agrega un encabezado al frente de cada segmento. Esta capa aplica un protocolo (conjunto de reglas), que pertenece a la capa.
Las tres capas inferiores del modelo OSI (transporte, red y enlace de datos) agrupan los datos y les agregan encabezados o avances (trailers).

PDU: Unidad de datos primaria. La PDU de la capa de transporte es el segmento:


**Segmento de la capa de transporte**

La capa de red convierte cada segmento en un paquete adjuntando otro encabezado. La PDU de la capa de red es el paquete:


Paquetes de la capa de red

La capa de enlace de datos convierte cada paquete en una trama, adjuntando un encabezado y un trailer:


La trama es transmitida a través del medio en forma de 0110010101

En el extremo receptor, los datos se deben desempaquetar. Las capas inferiores eliminan los encabezados y trailers, y la capa de transporte ensambla varios segmentos para crear el flujo de datos original y pasarlo a niveles superiores.

El proceso también es llamado encapsulación y desencapsulación.

## ¿Cómo funciona Internet?

### Protocolo de Internet (IP)

IP: Protocolo de Internet. Normas que rigen el intercambio de información a través de una red.

TCP: Transmission Control Protocol.

Ambos protocolos sientan las bases de Internet. El protocolo IP define una estructura de paquetes que agrupa los datos que se tienen que enviar. Así, establece la información sobre el origen y el destino de los datos y los separa de los datos útiles en la cabecera de cada paquete de información enviado.

El protocolo IP identifica cada dispositivo que se encuentra conectado a la red mediante su Dirección IP, la cual identifica unívocamente tanto al dispositivo como a la red a la que pertenece.

Quien se encarga de las traducciones entre nombres de dominio y direcciones IP es el protocolo de sistema de nombres de dominio —Domain Name System o DNS.

**Modelo de protocolos TCP/IP**

TCP/IP provee conectividad de extremo a extremo especificando cómo los datos deberían ser formateados, direccionados, transmitidos, enrutados y recibidos por el destinatario.

TCP: Protocolo de Control de transmisión. Permite la comunicación confiable entre computadoras. Garantiza el establecimiento de la conexión, la transferencia de datos y la finalización de la conexión.

IP: Protocolo de Internet. Permite enviar los datos en paquetes direccionables a las distintas computadoras de la red.

DHCP: Dynamic Host Configuration Protocol. Encargado de asignar las direcciones IP.

HTTP: Hypertext Transfer Protocol. Protocolo Cliente-Servidor, que gestiona las transacciones web. Sigue el esquema petición-respuesta entre un cliente y un servidor. La comunicación no está protegida, de forma que un tercero podría capturar los datos.

HTTPS:  Hypertext Transfer Protocol Secure. Encripta los datos enviados entre clientes y servidores.

URI: Uniform Resource Identificator. Dirección web.

URL: Indica dónde se encuentra el recurso que se desea obtener. Siempre inicia con un protocolo. Ej: http://www.
URN: Nombre exacto del recurso uniforme, el nombre del dominio y en ocsiones el nombre del recurso.

DNS: Domain Name System. Permite al servidor encargarse de la transformación URL a dirección IP.

ftp: Protocolo de transferencia de archivos.

SSH: Secure Shell. Protocolo para acceder a equipos remotos.

SMTP: Protocolo para transferencia de correo electrónico.

POP3 / IMAP: Protocolos para recepción de correos desde una casilla.

UDP: Protocolo de datagramas de usuario. Protocolo de nivel de transporte basado en el intercambio de datagramas. Su función es permitir el envío de

datagramas a través de la red sin que se haya establecido previamente una conexión. El protocolo UDP es más ligero ya que no utiliza tantas capas como el protocolo TCP/IP. El protocolo busca enviar los datos lo más rápido posible, sin tener en cuenta si el paquete llegó completo o no. Es utilizado para la transmisión de datos a alta velocidad como el streaming, videojuegos, etc.

Sincrónico:

https://view.genial.ly/60b299dcfafa9d0d8314a932

https://docs.google.com/document/d/1Gsk_T3dZSKnrNMFtT2GD6ZxCAliophyJZgMHQEIg8Fc/edit

Padlet:

https://padlet.com/PedagogiaDH/sed5su5teob8j5al

**Sesión 18.**

**Julio 8 de 2021.**

**Modelo OSI:**
https://view.genial.ly/60b299dcfafa9d0d8314a932

https://community.fs.com/es/blog/tcpip-vs-osi-whats-the-difference-between-the-two-models.html

**Capa de aplicaciones**
Capa con la que interaftúa el usuario final.

Error de capa 8: Es el usuario el que está haciendo algo mal.
Capa 6: Reconocimiento de datos, ej. HTML.
Capa 5: Se establece la sesión.

El protocolo define qué es lo que se va a hacer con el servidor. La comunicación se hace a través de direcciones IP. El puerto da información sobre la naturaleza de la petición.

Capa 4: Las capas 5, 6 y 7 especifican qué se va a hacer. La capa 4 especifica cómo lo vamos a hacer.

¿Cómo viaja la información en Internet?
https://www.youtube.com/watch?v=x3c1ih2NJEg

En TCP, por cada envío hay una respuesta. Si la respuesta no llega, se considera que el paquete se perdió y se vuelve a enviar. ("Se agotó el tiempo de conexión").
En UDP, no se garabtiza la llegada de la información.

Al hacer un ping se utiliza el protocolo TCP.

IP asegura que la conexión se haga, pero no de que llegue el mensaje; para eso existe en protocolo TCP. El IP es el protocolo que "ordena el camino"

Capas 3, 2 y 1 definen el dónde se hace.

Capa 1: ¿Por dónde sale? Ethernet, WiFi...

¿Qué? Capas 5, 6, 7.
¿Cómo? Capa 4.
¿Desde dónde hacia dónde? Capas 1, 2, 3.

**Sesión 19. Protocolos de Internet (Intermedio) II**

**Julio 12 de 2021**

## La famosa dirección IP

Número único que representa la ubicación cada dispositivo que se conecta a la red. En la actualidad es un número de 32 bits representado por cuatro cadenas de números, los cuales varían de 0 a 255 y se separan por puntos. Ejemplo:

192.168.32.1

Cada sección de la dirección se llama "octeto". Cada octeto está formado por 8 bits, y por tanto va de 0 a 255. La primera parte identifica la red, y la última parte identifica el host.

Direcciones clase A:
El número de red solo contiene un octeto y los otros tres corresponden la hosto.

Direcciones clase B:
Tanto el número de red como el host contienen cada uno dos octetos

Direcciones clase C:
El número de red contiene 3 octetos y el host 1.

Las IP públicas tienen que ser únicas. Las IP privadas pueden ser reutilizadas una y otra vez. Esta estrategia permite  sortear en parte la saturación del sistema IPv4.

Muchos fabricantes de Routers preconfiguran las direcciones 192.168.1.1 o 192.168.0.1

La IP privada también debe ser única; no puede repetirse dentro de la misma red. Dentro de la red, los dispositivos se identifican mediante su IP privada, pero al acceder a Internet se comunican a través del router, mediante una IP pública única.

Para conocer la IP pública:
Www.whatsmyip.com
179.13.151.69

Para conocer la IP privada:
ipconfig
192.168.1.55

## Direcciones MAC

MAC = Media Access control. Es un identificador único que cada fabricante le asigna a la tarjeta de red de sus dispositivos conectados, desde un ordenador o móvil hasta routers, impresoras u otros dispositivos. Cada dirección MAC es única a nivel mundial y, en teoría, son fijas para cada dispositivo.

Cada dirección MAC incluye seis parejas de números. Los primeros tres pares identifican al fabricante, y los otros tres identifican al modelo específico. Es común tener una dirección MAC para Ethernet, otra para wifi y otra para bluetooth.

Para averiguar el código MAC:
ipconfig/all

Ej: 01:3A:1D:54:6B:32

01:3A:1D: identificador único del fabricante (OUI)
54:6B:32: Identificador del producto (UAA)

**Direcciones IP**

IP estática: Aunque el dispositivo se apague, continúa teniendo la misma IP.
IP dinámica: Si el dispositivo se apaga, al encenderse puede tomar una nueva dirección IP.

Subred: Combinación de números que sirve para delimitar el ámbito de una red de computadoras. El protocolo TCP/IP usa la máscara de subred para determinar si un host está en la subred local o en una red remota.

Ej 255.255.255.0

Esta máscara indica que los tres primeros números corresponden a la re dy el último número al host.

**Direcciones IP importantes**

Router: La primera dirección disponible corresponde al router. Ej: 192.168.1.1.

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 de la red. Ej: 192.168.1.255.

**IPv6**

Ventajas:

- Número casi ilimitado de Ips únicas. Importante por el avance del Internet de las Cosas. IoT.
- Autoconfiguración.
- Más seguridad.
- Más eficiencia.

**Direccionamiento**

Routing (Enrutamiento): Mover datos de una red a otra.

Cuando se requieren diferentes servicios de un mismo sitio (por ejemplo Google), esto se logra a través de puertos. Cada dispositivo tiene 65536 puertos. Cada puerto está destinado a enviar o a recibir cierto tipo de información.

Puertos:
0 – 1023: Reservados para el Sistema Operativo y los protocolos de re dmás impotantes.
21: ftp
25: SMTP
80: HTTP

1024 – 49151: Puertos registrados que utilizan las aplicaciones instaladas. Son asignados por la Internet Assigned Numbers Authority (IANA).

Superiores a 49151: Puertos dinámicos o privados. Por ejemplo, cuando se navega una página web, se genera un puerto y cuando termina la navegación, este se libera.

Ej: Una solicitud a una página web (HTTP):
142.251.33.100:80

En ese caso se genera un puerto aleatorio en el computador, en el que se recibirá la información de respuesta.

**Enrutamiento**

Funciones del router:
- Recibir el paquete de datos.
- Buscar la dirección de destino.
- Verificar la tabla de enrutamiento configurada.
- Enviar el paquete destino por la mejor ruta posible.

Componentes de una tabla de enrutamiento:
- Red de destino
- Siguiente salto
- Interfaz de salida

Tipos de enrutamiento:

Estático: Las tablas se crean de forma manual.
- Consume menos ancho de banda
- Consume menos memoria
- Se utiliza para redes pequeñas
- No es escalable
- El mantenimiento es complicado

Dinámico: La información necesaria para crear y mantener actualizadas las tablas se obtienen de los demás routers de la red
- Alto consumo de ancho de banda
- Alto consumo de memoria
- Se utiliza para redes grandes
- Es automático

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

En un paquete de datos siempre se incluyen dos puertos: el del emisor y el del receptor.

Protocolo TCP: Conectivo, fiable y orientado a conexión. Garantiza la reposición de los paquetes que puedan perderse en la ruta.
Los protocolos HTTP, FTP y SSH de la capa de aplicación utilizan todos el protocolo TCP.

**Puertos TCP:**
Puerto 21: Conexiones a servidores FTP.
Puerto 22: Conexiones seguras SSH y SFTP.
Puerto 25: SMTP para envío de correos electrónicos. También se pueden usar los puertos 26 y 2525.
Puerto 53: Servicio DNS (Domain Name System).
Puerto 80: Navegación web de forma no segura HTTP.
Puerto 443: Navegación web segura HTTPS; utiliza el protocolo TLS por debajo.
Puerto 3306: Bases de datos MySQL.
Puerto 8080: Puerto alternativo al Puerto 80 TCP para servidores web. Normalmente se utiliza en pruebas.

**Sincrónico**

**Grupo examen:**
Octavio Dogil
Christian Borras Torres

Laura Anderson
Carlos Agudelo
Mauricio Pineda

**Tema:**
Procesos

El router puede hacer como switch y los switches se comunican a través de direcciones MAC

192.168.1.1 Administrador de la red?

Las IP por defecto usan IP dinámicas. Las empresas usan IP estáticas para ciertos dispositivos, porque necesitan identificarlos, por ej. Los servidores.
Ej: una impresora en red tiene que ser estática, para que todos los equipos lo puedan identificar, y para que no pierda su IP, por ejemplo, cuando se desconecta la Internet.
La Internet actual sobrevive porque se pueden hacer subredes.

Se puede tener la misma dirección IP pública, ya que representa la dirección IP.

Puerta de enlace predeterminada: Dirección IP del router.

Puerto 80: HTTP
Puerto 93: email

Node Dinamic IP

Establece servicio DNS
La IP es dinámica, solo trabaja el DNS.

Consultar puertos:
23
443
587
80
110
995
143
22
21
53
23
8080

Consultar protocolos:
HTTPS
HTTP
POP3
TCP
SMTP
IMAP
UDP
DHCP
DNS
IP
SSH
FTP

Padlet:
https://padlet.com/PedagogiaDH/t99h6vy3k0eugqzp

https://www.redeszone.net/tutoriales/configuracion-puertos/puertos-tcp-udp/

**Sesión 20. Protocolos de Internet (avanzado) III**

**Julio 14 de 2021**

Intranet, Extranet e Internet

Intranet es una red informática que utiliza los protocolos de Internet para compartir información, sistemas operativos o servicios de computación dentro de una organización.

Extranet: Es parte de la Intranet de una organización que se extiende a usuarios fuera de ella.

Internet: Se define como una red de redes, ya que conecta computadoras de todo el mundo.

ISP: Proveedor de Servicios de Internet.
Puede utilizar diferentes tecnologías: Fibra óptica / Banda ancha / Cable módem / 3G / 4G
Desde 2018, la mayoría de los datos viajan encriptados.

Proxy: Servicio informático que intercepta conexiones de red hechas desde un cliente a un servidor de destino eludiendo el ISP.

VPN: Red privada virtual. Es una tecnología que permite una extensión segura de la red local sobre una red pública como Internet. Permite que nuestra computadora envíe y reciba datos conectándose a otras redes compartidas o públicas como si fuera una red privada con toda la funcionalidad, seguridad y políticas que tiene una red privada.
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.

Tor: Red de anonimato que se encuentra distribuida y superpuesta sobre Internet. El direccionamiento de los mensajes no revela la dirección IP de los usuarios. Además, mantiene la integridad y el secreto de la información que viaja por ella.
Donde las VPN brindan privacidad, Tor brinda anonimato.

**Sincrónico**

El router utiliza el protocolo DHCP para asignar las IP dinámicas a los dispositivos.

El router permite manejar IP para conectarse a Internet, mientras que en las redes privadas se utilizan los switches.

Los saltos de red los hace el protocolo IP.

VPN: OpenVPN
Otras: Windscribe

Tor encripta la información en cada salto de red que se hace. Tor además oculta la IP.

Las páginas en la Deep Web y en la Dark Web son muchas veces HTML plano.

Las páginas web en la Dark Web tienen formato .onion, lo cual hace que no estén indexadas. Si no se tiene el link, no se puede entrar.

Proxy: Puede ser un dispositivo físico o puede ser configurado en una computadora. Toda los dispositivos de la red se conectan al Proxy. El Proxy pone una barrera que filtra la información que puede llegar a la red.

Un farewell se configura en una computadora, mientras que el Proxy lo hace para la red.

Existe otro tipo de teconología, llamada DMZ, que es en cierta forma inversa a la DMZ. Puede bloquear todas las peticiones, excepto las que se especifiquen. Es una técnica efectiva contra los Ataques de Denegación de Servicio y los Ataques de Denegación de Servicio Distribuida. En los primeros, todas las peticiones vienen desde una misma región, mientras que en las segundas los ataques viene desde todo el mundo.

El Proxy en general es un software que corre en el servidor

https://thehiddenwiki.org/

.onoin: Enmascara las direcciones IP y encripta la información.

Padlet:
https://padlet.com/PedagogiaDH/pyzk7qtf75yws0kt

**Sesión 21**

**Sincrónico**

IP es el protocolo que busca el mejor método de enrutamiento.

Repaso: Domingo, 4,00 pm. Aula 43.