

REDES DE COMPUTADORES Y LABORATORIO

Christian Camilo Urcuqui López, MSc



LÍNEAS DE TRABAJO

Semillero de investigación
en ciberseguridad




1. Detección de malware en dispositivos Android
2. Detección de ciberataques web
3. Detección de páginas web maliciosas
4. Controles de seguridad para *Defacement*
5. *Hacking* con hardware
6. Detección de mineros de criptomonedas.
7. Seguridad para la inteligencia artificial (Adversarial Machine Learning)

PROYECTOS DE INVESTIGACIÓN





1. Blockchain como herramienta de detección de intrusiones.
2. El caballo de Troya de nuestra época: Botnets.
3. Metodología de garantizar la seguridad en routers
4. Una mirada más modesta al cryptojacking
5. MIM: La inseguridad acechando
6. TOR: ¿sinónimo de anonimato?
7. ¿Llega a ser WhatsApp lo suficientemente seguro como se piensa?
8. WiFi Pineapple – Pineapple in the middle.


Grupos de 3 personas


 **urcuqui** Update Readme.md

Latest commit 4432639 2 minutes ago

..

 09711-RedesComunicacionesyLab.pdf	Create 09711-RedesComunicacionesyLab.pdf	6 days ago
 Readme.md	Update Readme.md	2 minutes ago
 Sesion1.pdf	corrección MAN->WAN	5 days ago
 Sesion2.pdf	Create Sesion2.pdf	4 days ago

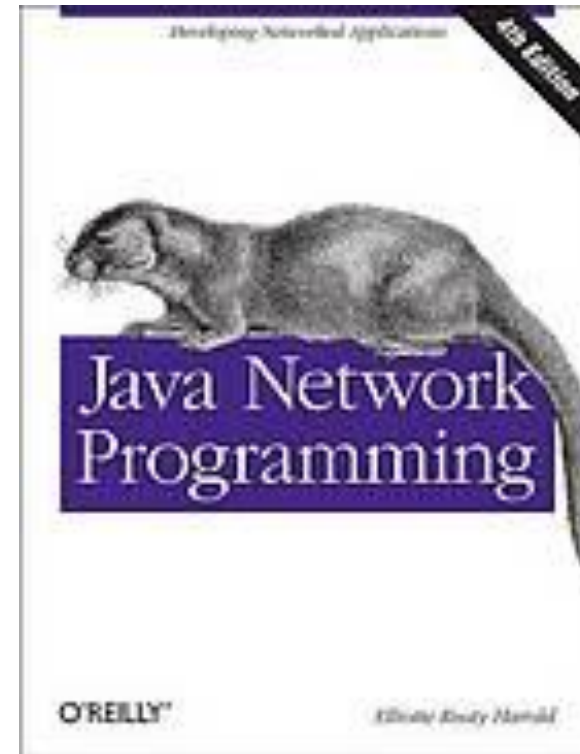
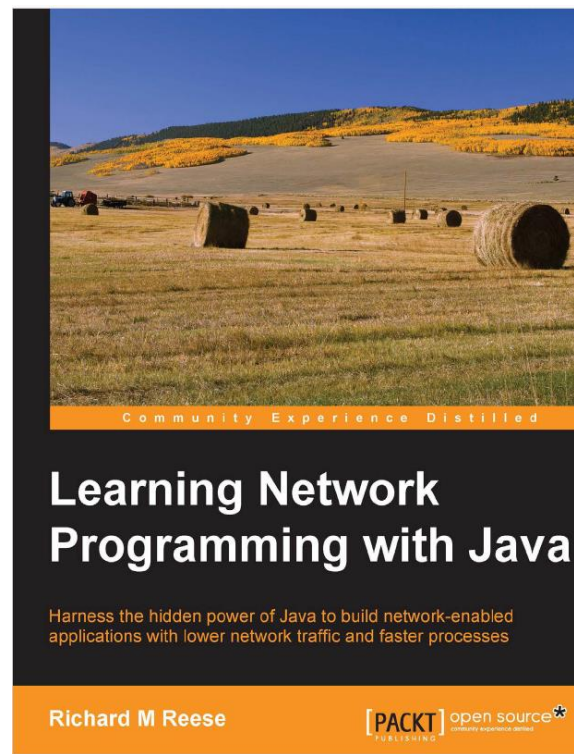
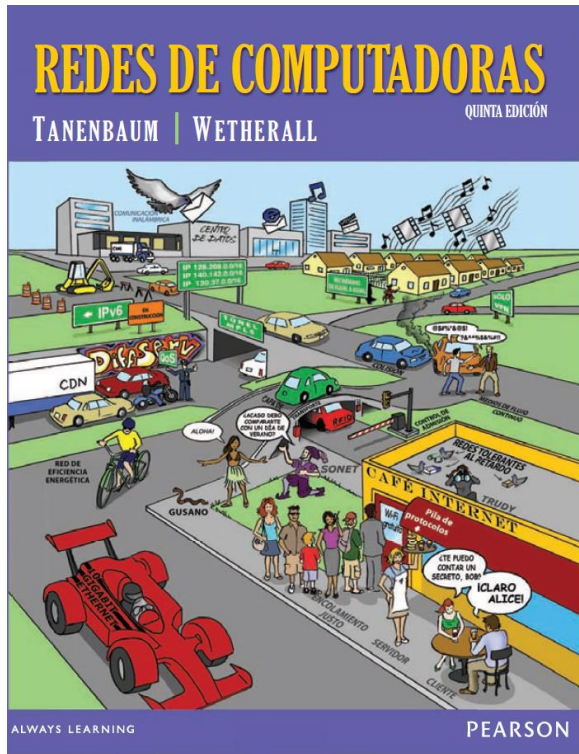
 **Readme.md**



Proyectos asignados

- Blockchain como herramienta de detección de intrusiones.
Grupo 1: Sebastian Arango Vergara, Steven Ma Mei, Daniel Galvis Torres
- El caballo de Troya de nuestra época: Botnets.
- Metodología de garantizar la seguridad en routers
- Una mirada más modesta al cryptojacking
- MIM: La inseguridad acechando
- TOR: ¿sinónimo de anonimato?
- ¿Llega a ser WhatsApp lo suficientemente seguro como se piensa?
- WiFi Pineapple – Pineapple in the middle.

BIBLIOGRAFÍA



PREGUNTAS

- ¿Repaso?
 - Redes punto a punto vs redes basadas en servidor
 - ¿Cómo funcionan los protocolos? Emisor y receptor.
- Explique el modelo de referencia OSI (capa 1-3)
- Explique el modelo de referencia OSI (capa 4-6)
- Explique TCP/IP
- Describa IP, TCP, UDP, ICMP, los dos tipos de demonios, FTP y Telnet.
- ¿Qué es una dirección IP, un nombre de dominio y un puerto?

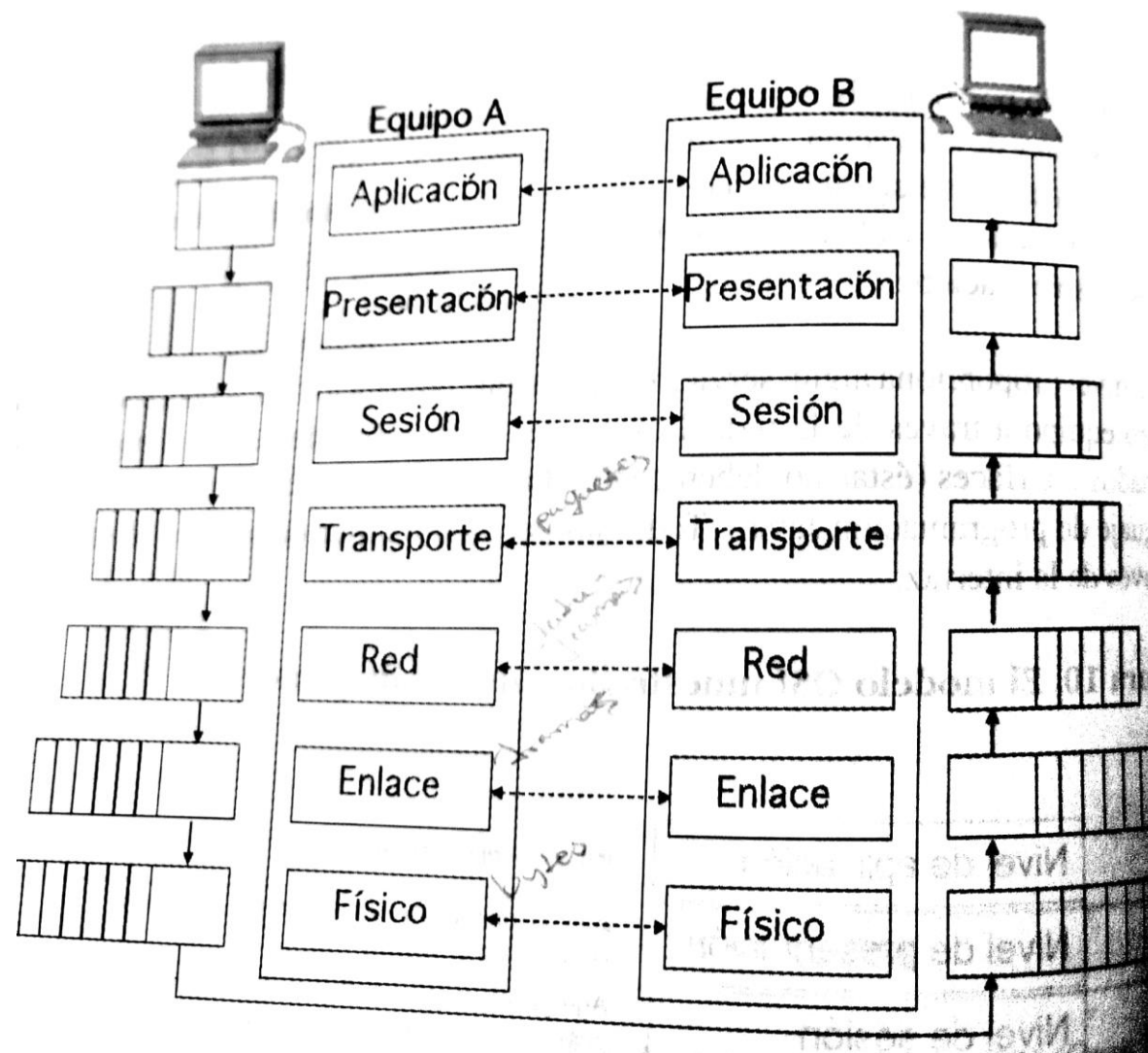


Figura 1. Comunicación entre niveles de OSI

NIVELES DEL MODELO OSI

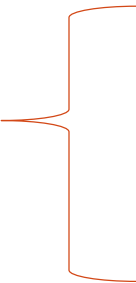

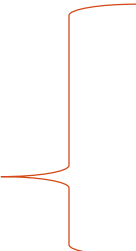
En el emisor

- Cada nivel de OSI el software agrega información de control adicional al mensaje, información necesaria para su correcta transmisión a través de la red. Por otra parte, en el receptor el mensaje es procesado en el orden inverso.

En el receptor

- Existe un software por cada nivel encargado de leer la información del mensaje, desglosarlo y pasarlo al nivel superior.
- Cuando los datos llegan a la capa de aplicación (nivel 7) ya toda la información de control se ha eliminado y el mensaje se encuentra en su forma original, resultando legible para el receptor.

LAS PILAS DE PROTOCOLOS

Aplicación		Nivel de aplicación	Inicia o acepta una petición
		Nivel de presentación	Agrega información de formato, presentación y codificación al paquete
		Nivel de sesión	Agrega información de flujo de tráfico para determinar cuándo se enviará el paquete
Transporte		Nivel de transporte	Agrega información sobre el control de errores
Red		Nivel de red	Agrega al paquete información sobre dirección y secuencia
		Nivel de enlace	Agrega información de comprobación de errores y prepara los datos para la conexión física
		Nivel físico	Envía los paquetes como una secuencia de bits

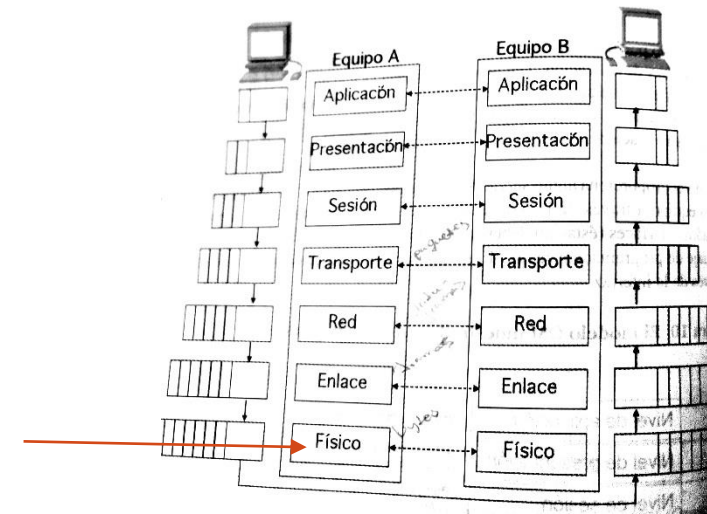
NIVEL FÍSICO

Nivel 1

Este nivel es el encargado de establecer el circuito físico para que la información pueda ser transmitida entre el emisor y el receptor. La unidad de información que manipula son los **BITS (ceros y unos)**.

Es el encargado de definir las características físicas, eléctricas, funcionales y procedimentales para establecer, mantener y desconectar el enlace físico. Estas características están relacionadas con:

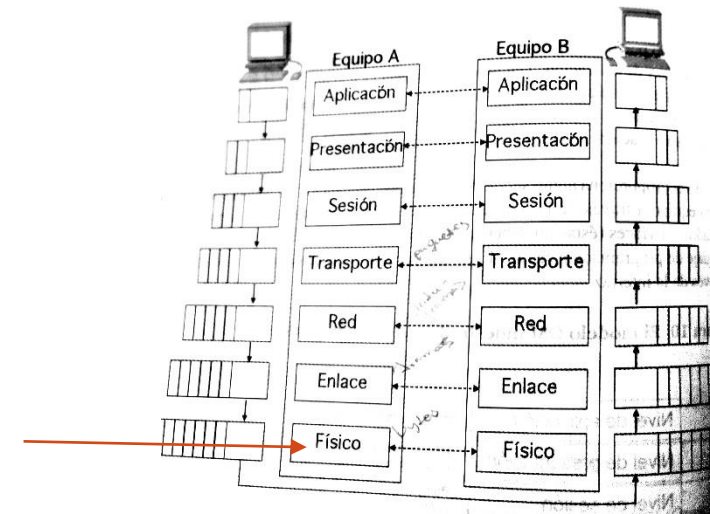
- La descripción de los cables y conectores.
- El número y uso de los pines de cada conector.
- Cómo se conecta el cable a la tarjeta adaptadora de red.



NIVEL FÍSICO

Nivel 1

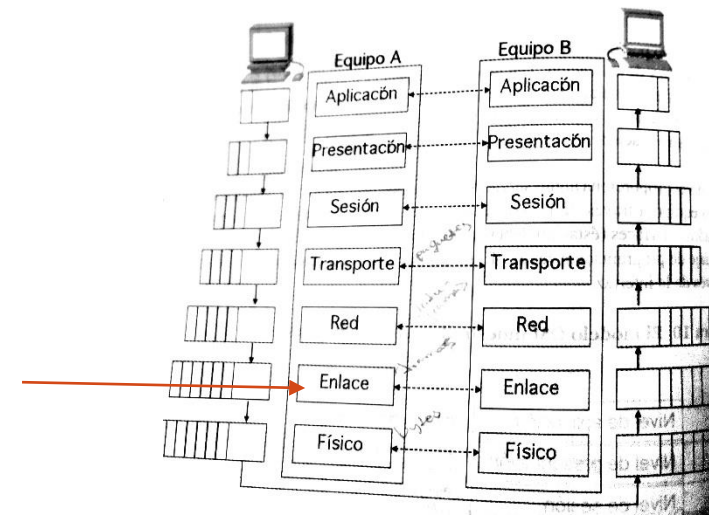
- Especificación eléctrica, nivel de señal e impedancia.
- Sincronización de bits



ENLACE DE DATOS

Nivel 2

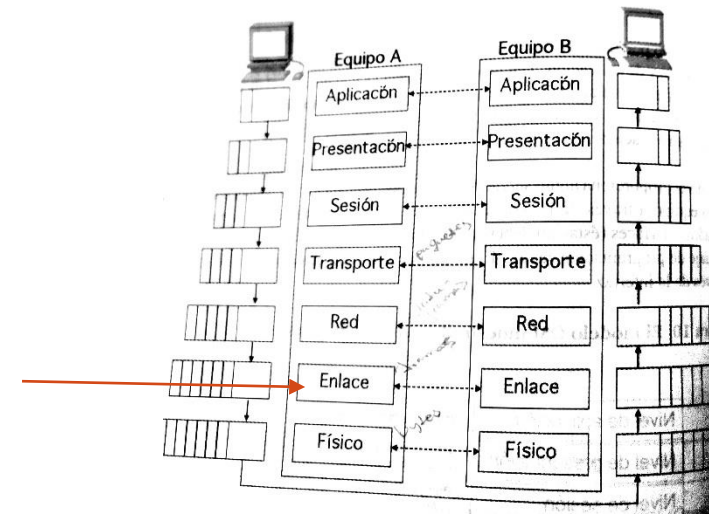
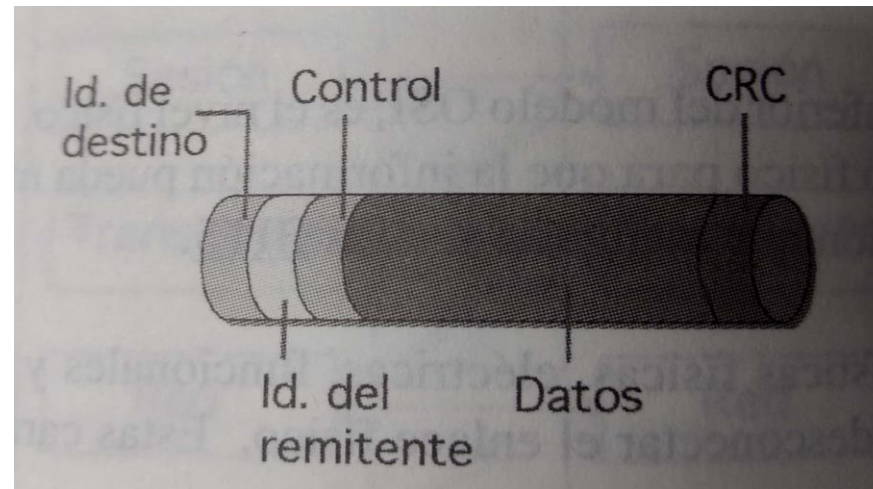
- El nivel tiene como objetivo proporcionar una transmisión libre de errores y de realizar el acceso al medio de comunicaciones. La unidad que se maneja son las **TRAMAS**.
- En el emisor se envían las tramas de datos desde el nivel de red al nivel físico y en el receptor se empaquetan los bits en bruto desde el nivel físico a tramas de datos.



ENLACE DE DATOS

Nivel 2

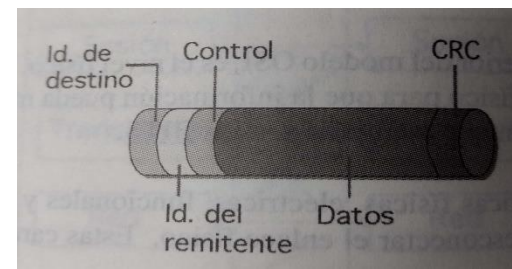
- Una trama de datos es una estructura compuesta por los datos de la comunicación y la información de control.



ENLACE DE DATOS

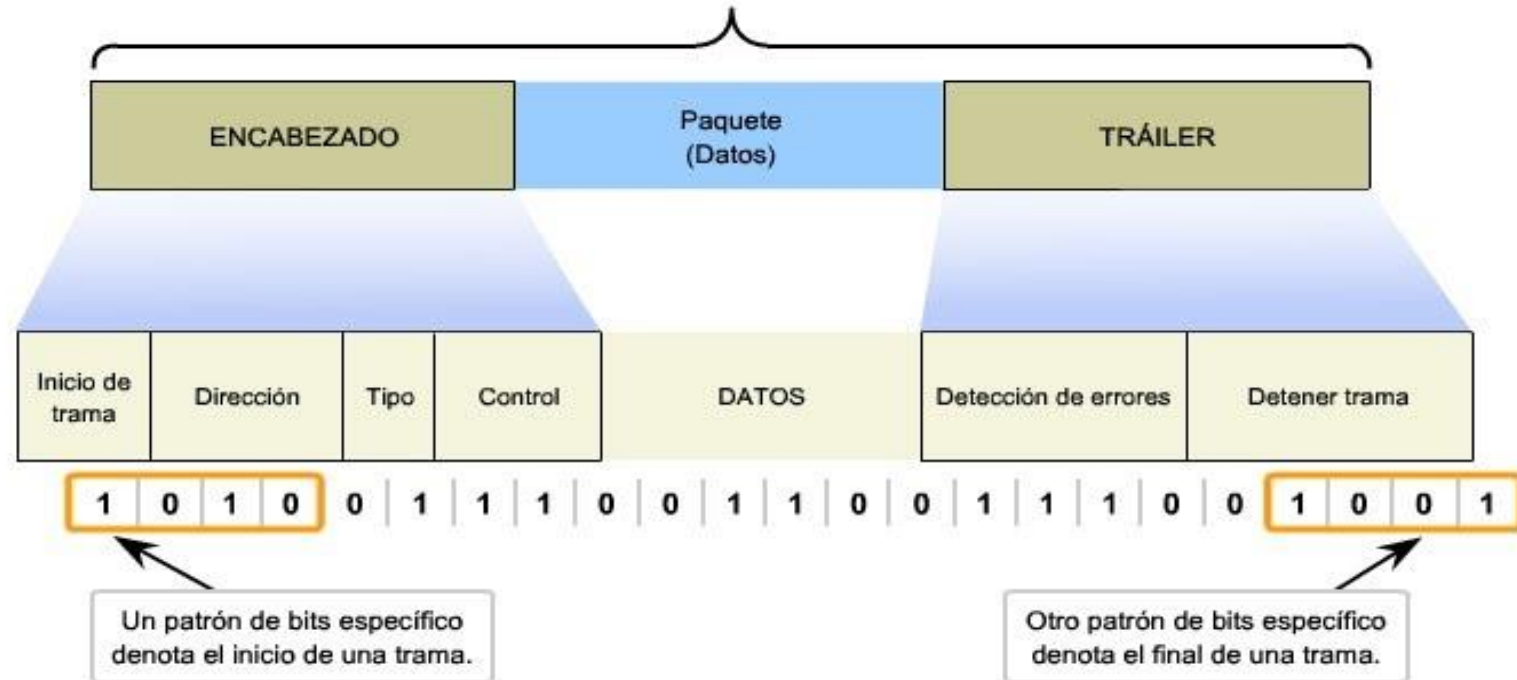
Nivel 2

- Identificación del destino y del remitente (ambas son representaciones de las direcciones de los equipos).
- La información de control que se usa para la información del tipo de trama, el **enrutamiento y segmentación**.
- La comprobación de **redundancia cíclica (CRC, Cyclic Redundancy Check)** es la información que contiene la corrección de errores y de comprobación para asegurar que la trama de datos se recibe correctamente.



ENLACE DE DATOS

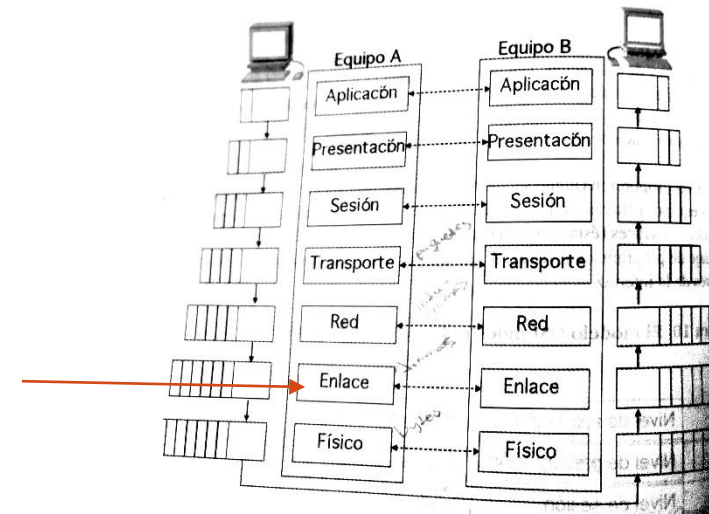
Formateo de datos para la transmisión



ENLACE DE DATOS

Nivel 2

- Retransmisión y corrección de errores en la transmisión.
- Supervisión de la conexión física
- En este nivel se habla de direcciones **MAC (Medium Access Control)** de los adaptadores de red, “las cuales son únicas” y vienen grabadas en el adaptador o tarjeta de red.

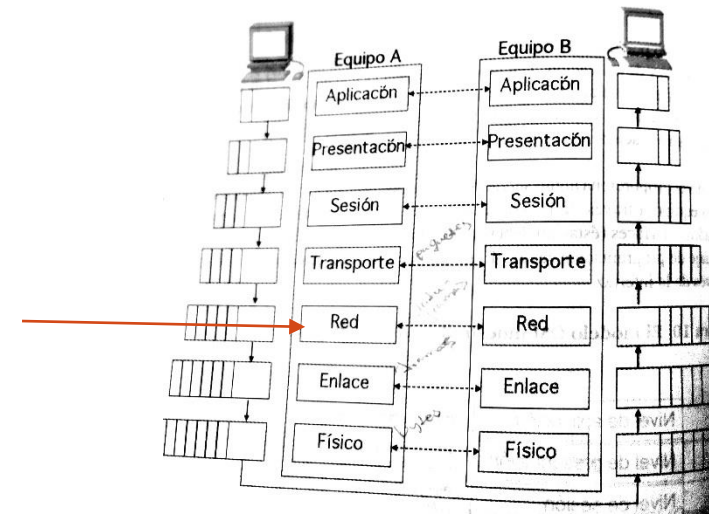


NIVEL DE RED

Nivel 3

Es el responsable del direccionamiento de los mensajes y la conversión de las direcciones y nombres lógicos a direcciones físicas. **Determina el enrutamiento el emisor y el receptor.** Determina qué trayectoria deben seguir los datos con base en las condiciones de la red, la prioridad del servicio y otros factores.

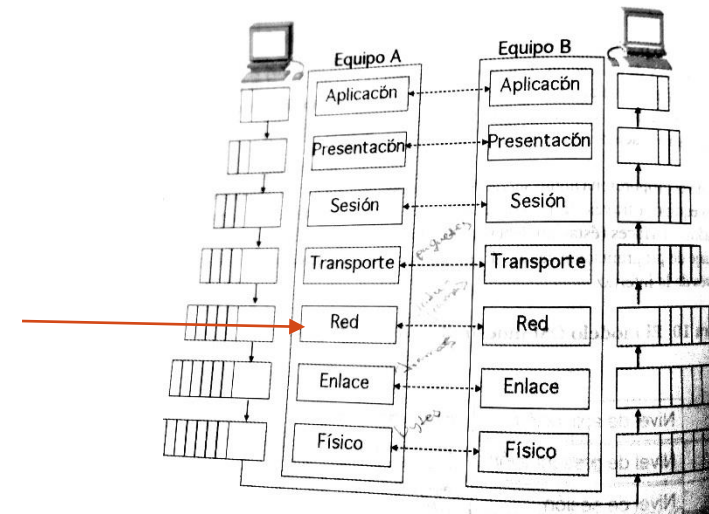
La unidad que se maneja en este nivel son los **DATAGRAMAS**.



NIVEL DE RED

Nivel 3

- Encargado de administrar los problemas de tráfico de la red, tales como la conmutación de paquetes, el enrutamiento y el control del tráfico de datos.
- En este nivel se habla de ***direcciones lógicas*** para identificar cada equipo dentro de la red.



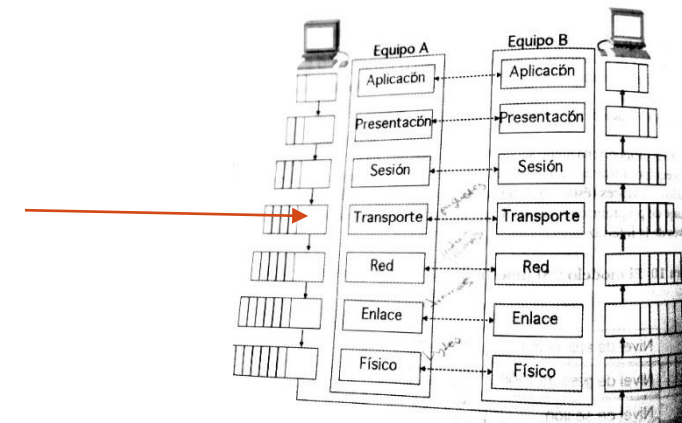
NIVEL DE TRANSPORTE

Nivel 4

La principal tarea de esta capa es establecer, controlar y liberar las **conexiones de transporte**, las cuales son conexiones de extremo a extremo entre los sistemas de comunicaciones.

La unidad que se maneja son los **PAQUETES** o **SEGMENTOS**.

Este nivel aísla las capas superiores de los detalles relativos a los servicios de comunicación. Se encarga de proporcionar un canal de comunicaciones libre de errores. Asegura que los paquetes se entreguen sin errores, secuencialmente y sin pérdidas o duplicaciones.



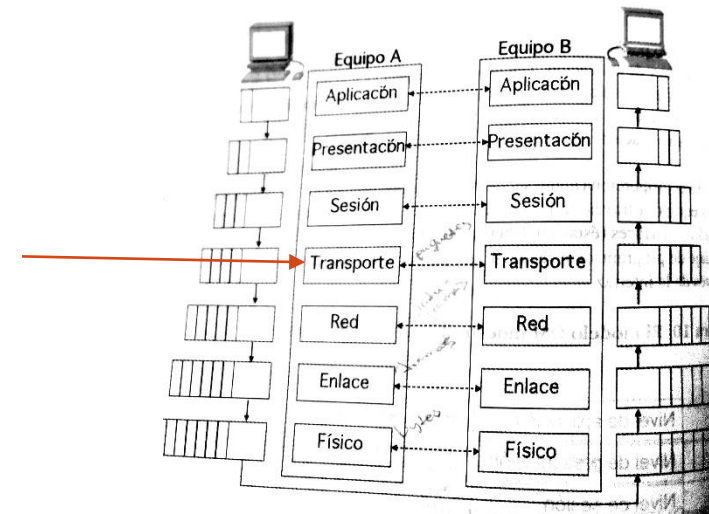
NIVEL DE TRANSPORTE

Este nivel re-empaqueta los mensajes, es decir, divide los mensajes grandes en varios paquetes y colocando los paquetes pequeños juntos en un paquete grande. Esto permite que mejore la eficiencia de la transmisión sobre la red. Usualmente, el nivel de transporte del receptor desempaqueta los mensajes, vuelve a montar el dato original y envía una señal de confirmación al emisor.

El nivel de transporte proporciona control de flujo, control de errores y participa en la solución de problemas relacionados con la transmisión y recepción de paquetes.

NIVEL DE TRANSPORTE

- El **control de flujo** se refiere a la regulación del flujo de información, con el objetivo que los equipos intercambien información a la “misma velocidad” y que un equipo rápido no pueda saturar a uno lento

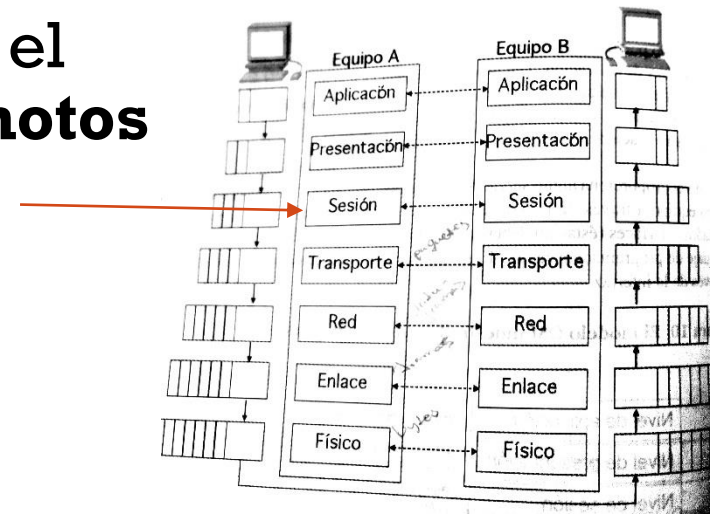


NIVEL DE SESIÓN

Nivel 5

Establece y termina la relación de la comunicación en una forma ordenada, aspecto que se denomina ***Servicio de administración de la sesión***.

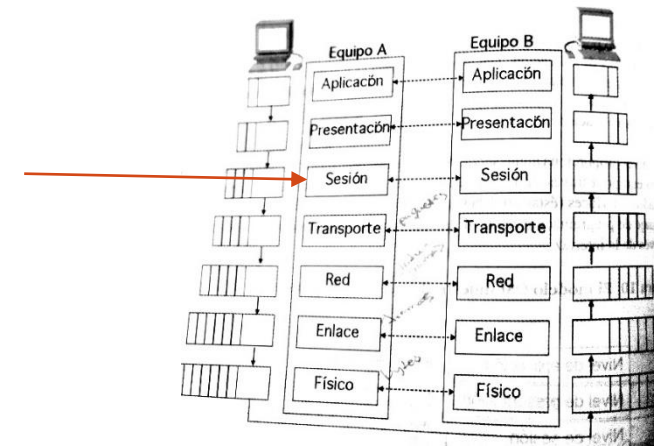
Una sesión se establece cada vez que un equipo de la red necesita utilizar los recursos informáticos de otro. La capa de sesión actúa como interfaz entre el usuario y la red, gestionando el establecimiento de la conexión entre **procesos remotos**



NIVEL DE SESIÓN

Nivel 5

El nivel de sesión proporciona la **sincronización entre tareas de usuarios**, colocando puntos de control en el flujo de datos. De esta forma, si la red falla, sólo es preciso retransmitir los datos posteriores al último punto de control. Este también es el encargado de llevar el control del dialogo entre los procesos de comunicación, regulando que lado transmite, cuándo y por cuánto tiempo.

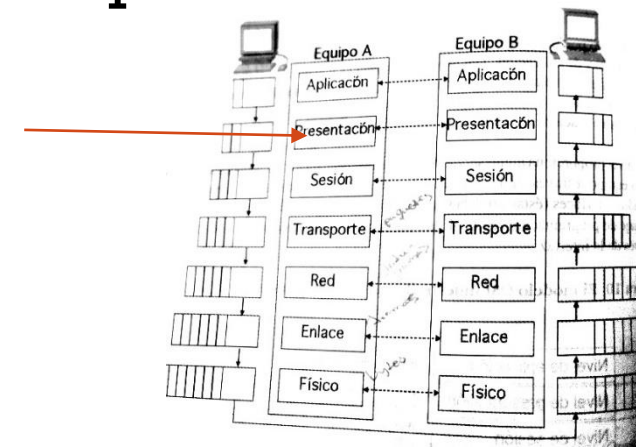


NIVEL DE PRESENTACIÓN

Nivel 6

Es el encargado de definir el formato de los datos intercambiados entre los procesos que dialogan (se podría definir como el traductor de la red).

En el emisor la capa 6 convierte los datos desde un formato por el nivel de aplicación a otro formato intermedio reconocido. Este nivel en la capa del receptor convierte el formato intermedio a uno que sea entendible por el nivel de aplicación de ese equipo.



NIVEL DE PRESENTACIÓN

Permite hacer que el usuario no se entere de las dificultades que pueden existir cuando se comunican equipos heterogéneos, por ejemplo:

- Diferente longitud de palabra.
- Distintos códigos de caracteres en el computador fuente (origen).
- Distintas representaciones de la información.
- Este nivel puede aplicar **compresión de datos** para reducir la cantidad de bits a transmitir.

NIVEL DE PRESENTACIÓN

Es la única capa que no es transparente al usuario, es decir, el usuario la utiliza para su interacción con el software y el hardware subyacente a la red.

Se encarga de llevar servicios de red al usuario final, por ejemplo:

- Transferencia de archivos.
- Conexión remota a otros sistemas.
- Correo electrónico

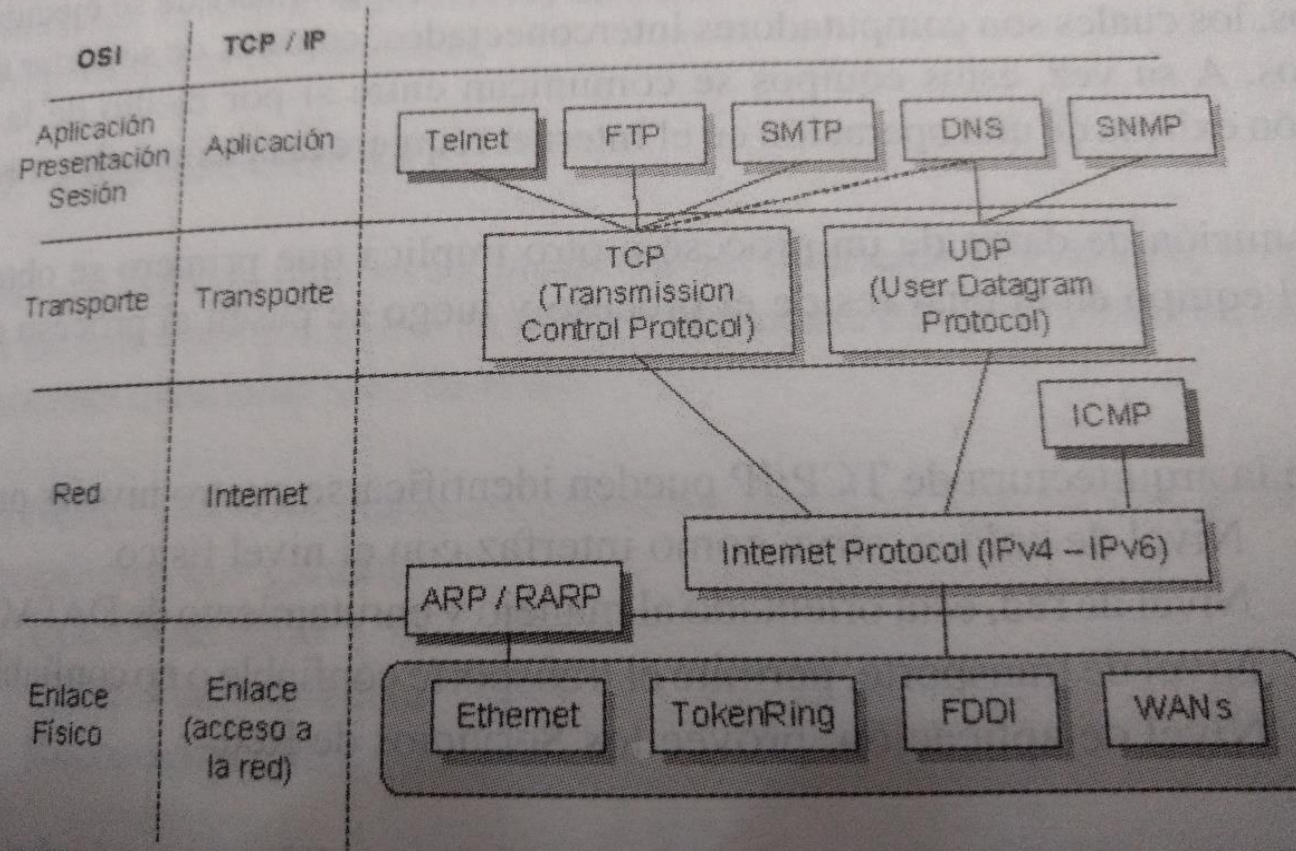
PILA DE PROTOCOLOS TCP/IP

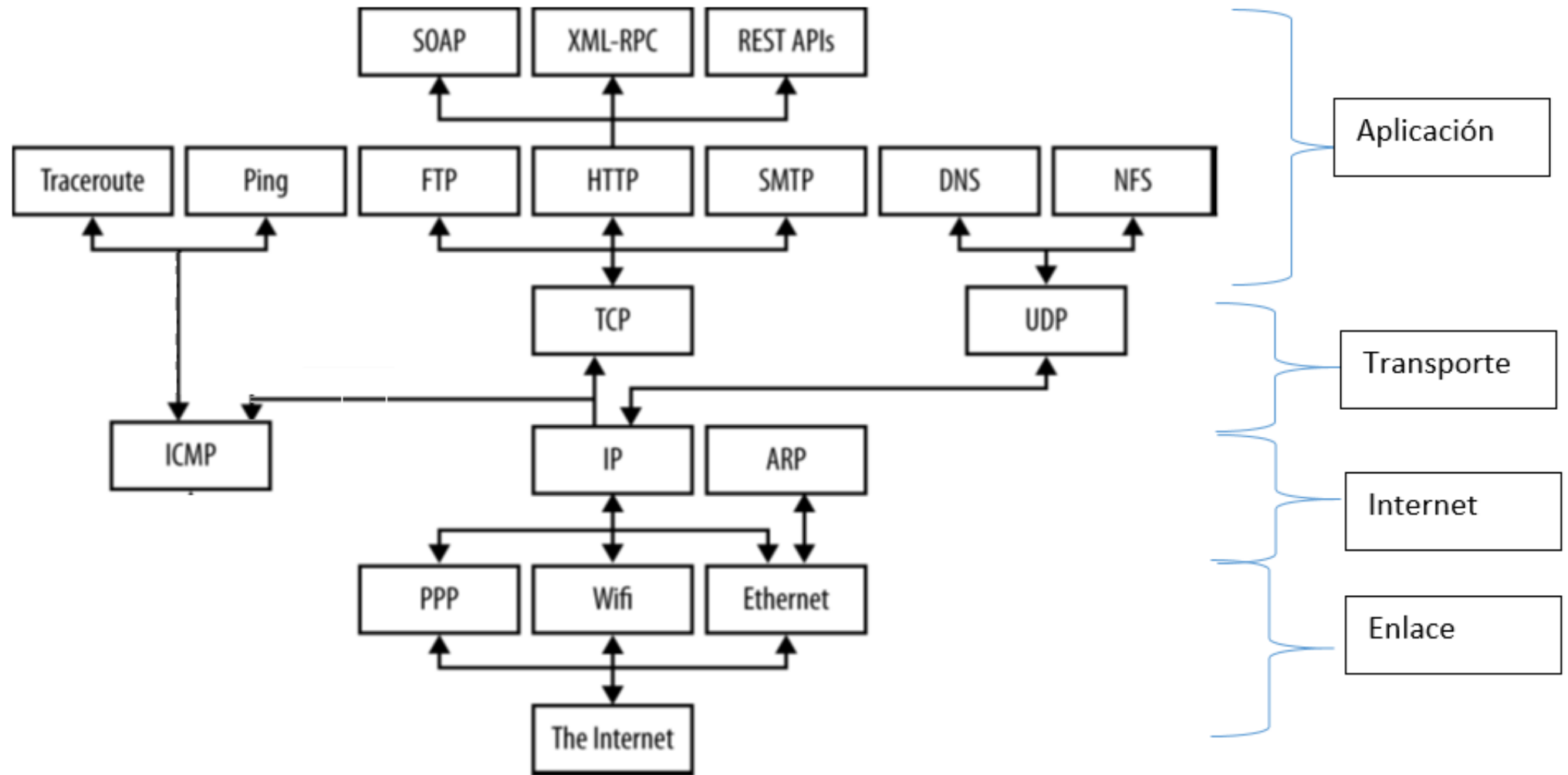
- **TCP/IP es una pila de protocolos** desarrollada por una comunidad de investigadores relacionados con la Agencia Estadounidense de Proyectos Avanzados de Investigación (ARPA – Advanced Research Projects Agency) en los años 70, la cual buscaba lograr que las redes de investigación de todo el mundo pudieran unirse para formar una sola red virtual llamada ARPANET.

PILA DE PROTOCOLOS TCP/IP

- TCP/IP (Transmission Control Protocol/Internet Protocol) es un modelo de referencia que se divide en cuatro capas apropiado para Internet.
- Todas las aplicaciones como Chrome y GitHub corren sobre la capa de aplicación y únicamente se comunica con la capa de transporte, del mismo modo la capa de transporte solo se comunica con la de Internet. Finalmente, la capa física transporta los datos entre nodos a través de cables, señales, cables de fibra óptica.

Figura 13. Niveles OSI vs. niveles TCP/IP





TCP/IP – NIVEL DE ENLACE

Generalmente se encuentra conformado por la tarjeta de red correspondiente al computador y el software necesario para enlazar la tarjeta con el sistema operativo, las cuales actúan en conjunto para manejar el intercambio de datos entre un equipo, la red a la cual se encuentra conectado y otro equipo dentro de la misma red.

TCP/IP – NIVEL DE INTERNET

Es la capa encargada del movimiento de los paquetes a través de la red. Los protocolos de este nivel proporcionan servicios que permiten que los datos se intercambien entre equipos residentes en múltiples redes.

El protocolo de enrutamiento Internet no sólo se ejecuta en el equipo local, sino también en gateways que conectan dos redes.

Los protocolos IP (Internet Protocol) y ARP (Address Resolution Protocol) son los principales de este nivel.

PROTOCOLO IP

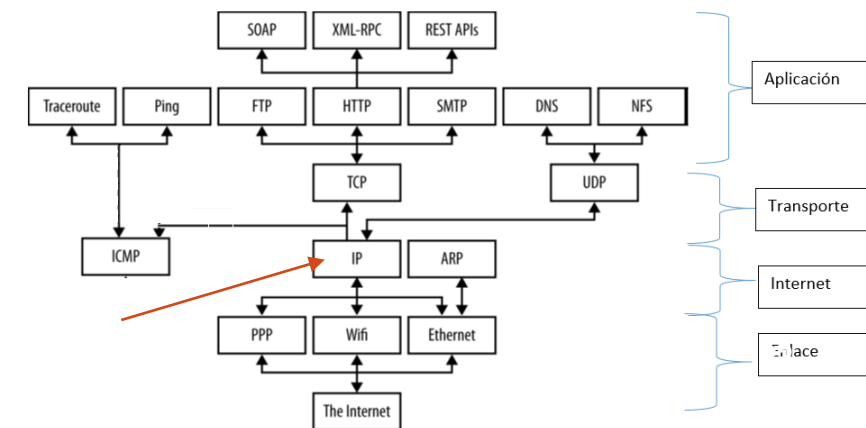
Internet Protocol, es un protocolo no orientado a conexión, responsable del enrutamiento de los datagramas que se transmiten de un emisor a un receptor.

En este protocolo no se garantiza:

- Control de flujo
- Control de secuencia
- Reconocimientos

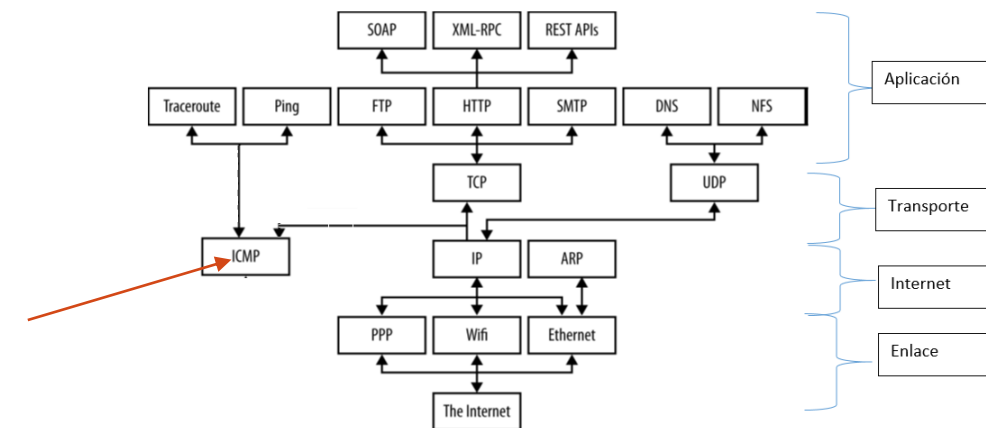
IPv4 – 32 bits

IPv6 – 128 bits



PROTOCOLO ICMP

- ICMP (Internet Control Message Protocol). Es un protocolo que utiliza IP con la finalidad de transmitir información de control y de errores acerca de las transmisiones de paquetes IP (datagramas).
- Por ejemplo, si un enrutador no puede enviar un datagrama IP, utiliza ICMP para informarle al emisor del mensaje que hay un problema.




```
Applications ▾ Places ▾ Terminal ▾ Mon 22:42 1 [system icons]
root@kali: ~
File Edit View Search Terminal Help
root@kali:~# ping 8.8.8.8
PING 8.8.8.8 (8.8.8.8) 56(84) bytes of data.
64 bytes from 8.8.8.8: icmp_seq=1 ttl=128 time=190 ms
64 bytes from 8.8.8.8: icmp_seq=2 ttl=128 time=106 ms
64 bytes from 8.8.8.8: icmp_seq=3 ttl=128 time=116 ms
64 bytes from 8.8.8.8: icmp_seq=4 ttl=128 time=137 ms
64 bytes from 8.8.8.8: icmp_seq=5 ttl=128 time=136 ms
64 bytes from 8.8.8.8: icmp_seq=6 ttl=128 time=169 ms
^C
--- 8.8.8.8 ping statistics ---
6 packets transmitted, 6 received, 0% packet loss, time 5010ms
rtt min/avg/max/mdev = 106.628/142.997/190.879/29.057 ms
root@kali:~#
```

TCP/IP – NIVEL DE TRANSPORTE

Proporciona un flujo de datos entre dos equipos, para el nivel superior. Asegura la confiabilidad y la integridad de los datos entre dos equipos TCP/IP, es decir, es el encargado de gestionar los datagramas sin procesar debido a los inconvenientes presentados en el envío (no se garantizan ya que pueden estar corruptas en el tránsito).

Los dos protocolos que conforman esta capa son:

- TCP (Transmission Control Protocol)
- UDP (User Datagram Protocol).

TCP/IP – NIVEL DE APLICACIÓN

En este nivel se ejecuta el procesamiento final sobre los datos según la “operación” que se desee realizar sobre ellos.

Algunos protocolos:

- SMTP, transferencia de correo electrónico
- FTP, transferencia de archivos
- SNMP, administración de red
- Telnet, para login remoto

TCP/IP — NIVEL DE APLICACIÓN

Demonios, procesos remotos

- Stand-alone
- Servidor, divide la tarea en dos procesos: Padre e hijo.

TCP/IP – NIVEL DE TRANSPORTE

Proporciona un flujo de datos entre dos equipos, para el nivel superior. Asegura la confiabilidad y la integridad de los datos entre dos equipos TCP/IP, es decir, es el encargado de gestionar los datagramas sin procesar debido a los inconvenientes presentados en el envío (no se garantizan ya que pueden estar corruptas en el tránsito).

TCP es un protocolo confiable orientado a conexión, para su uso en aplicaciones con grandes cantidades de datos y que requieren un reconocimiento de los datos recibidos.

UDP provee comunicaciones no orientadas a conexión y no garantiza la entrega de paquetes, no es un protocolo confiable debido a que no se puede verificar el orden de llegada de los datos al receptor.

COMPETENCIAS, PRÓXIMA CLASE

- Explicar el direccionamiento en Internet
- Describir DNS
- Aplicar los Factory methods de la API de Java

LECTURAS

Material utilizado	<p>1. Arboleda, L. (2012). Programación en Red con Java.</p> <p>2. Harold, E. (2004). Java network programming. " O'Reilly Media, Inc.".</p> <p>3. Tanenbaum, A. S. (2003). Redes de computadoras. Pearson educación.</p>
Actividades DESPUÉS clase	<p>A1. Revisar el contenido del libro 1 desde la página 35 hasta la 54</p> <p>A2. Leer del libro 2 el capítulo 2(opcional)</p>

REFERENCIAS

- <https://sites.google.com/site/cursoonlineaccna1//rsrc/1472866878047/unidad-4-capa-de-enlace-de-datos/4-1-capa-de-enlaces-de-datos-acceso-a-los-medios/4-1-3-capa-de-enlace-de-datos-creacion-de-una-trama/4.1.3.2.jpg>