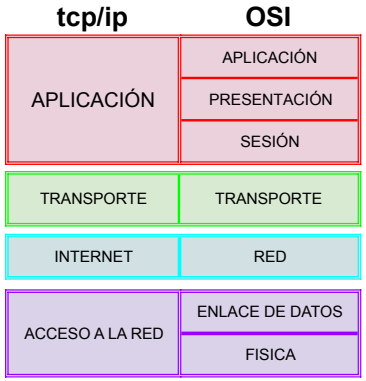
1. Dibuja los modelos OSI y TCP/IP e indica mediante colores la equivalencia de los niveles de ambos modelos.



2. Indica los puertos y protocolos de capa de transporte que usan los siguientes protocolos: HTTP, HTTPS, DNS, SSH

	PUERTO	PROTOCOLO
HTTP	80	TCP
HTTPS	443	TCP
DNS	53	TCP/UDP
SSH	22	TCP

3. Explica y razona cómo realiza la retransmisión de los paquetes el protocolo UDP, cuando no se ha recibido un ACK pasados "5 tics"

UDP es un protocolo no orientado a la conexión y por lo tanto no confiable, por lo que todos los datos que se pierden o no llegan a su destino pasados "5 tics" son desechados y no hay una retransmisión.

4. ¿Qué máscara de red (la más ajustada) debería usar si quiero disponer de, al menos, 63 máquinas conectadas a la red?

255.255.255.128 con 128 IPs disponibles de las cuales 126 son utilizables

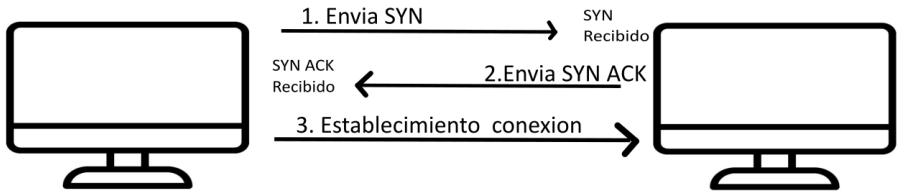
5. Explica detalladamente (y dibuja) como se establece una conexión TCP.

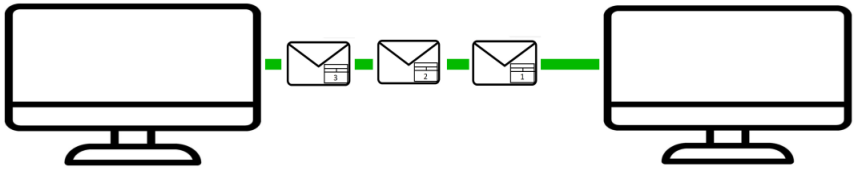
TCP es un protocolo orientado a la conexión, por lo que antes de enviar data al destino, los 2 host se comunican para establecer una conexión.

_ Provee una conexión fiable, esto significa que si un segmento no fué enviado, por cual sea la razón, volverá a ser enviado.

_ Provee en el encabezado un nro de secuencia que permite los segmentos ser enviados en orden.

_ Provee control de flujo, significa que el destinatario puede decir al remitente que disminuye o incrementa el flujo de data





6. Representa la IP 192.168.1.23 con máscara 255.255.192.0 en notación CIDR

_192.168.1.23/18

7. Define, con tus propias palabras, los siguientes conceptos:

a. Switch: Sirven para conectar diferentes hosts dentro de una LAN, trabajan dentro de la 2da capa del modelo OSI dado que para poder redirigir los datos primero aprende las direcciones MAC y de esa manera dirigir el tráfico de una manera eficiente

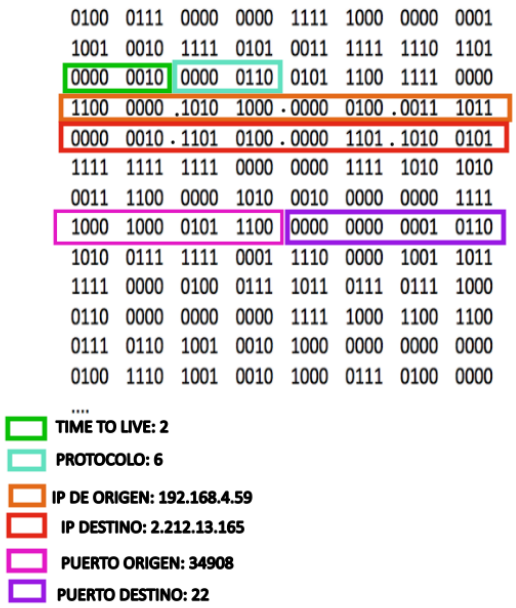
b. Router: Dispositivo que trabaja en la 3ra capa del modelo OSI, utiliza direcciones IP para identificar cada network a la que se conecta y así permitir a los dispositivos conectarse a internet. Cuando recibe paquetes identifica el destino y calcula la manera mas rapida de que llegue.

c. Firewall: sistema diseñado para evitar el acceso no autorizado a la red privada, bloquea tráfico no deseado y permite el que sí lo es. Su principal propósito es crear una barrera de seguridad.

d. NAT: (Traducción de direcciones de Red) es utilizado por los routers y lo que hace es modificar la fuente y/o destino de las direcciones IP, ayuda a preservar la limitada cantidad de direcciones IPv4 al permitIr múltiples host dentro de una red privada compartir una misma dirección pública.

8. Dado el siguiente paquete IP (paquete teórico), indica cual es que direcciones IP y puertos se están comunicando, así como el protocolo de capa 7 que se seguramente se

esté empleando. Además, indica cuántos “saltos” dará el paquete antes de descartarse.



9. Dada la red 192.160.0.0/11, indica y razona:

. **La máscara de red:** 11111111 11100000 00000000 00000000 = 255.224.0.0

. El número de host disponibles: 2097150

La dirección de broadcast: 192.191.255.255

Calcula si 192.191.13.80 y 192.168.90.45 están en la misma red: Si porque desde el host minimo es 192.160.0.1 y el host Maximo es 192.191.255.254

por lo tanto todas las IP dentro del rango del Host minimo y maximo pertenecen a la misma red que son el caso de 192.191.13.80 y 192.168.90.45

10. Enumera y explica detalladamente (con tus propias palabras) todos los ataques de red que conoces, tanto para IPv4 como para IPv6

1.IP SPOOFING: Proceso en el cual se disfraza el IP origen con una falsa

2. MITM(Hombre en el Medio): tipo de ciberataque en el que el hacker intercepta la conexión o envio de informacion entre dos dispositivos poniendose en el medio haciéndose pasar por uno de los dispositivos

3: Envenamiento ARP: técnica hacking que consiste en infiltrarse en una red y engañar a los dispositivos haciéndose pasar por la IP del destino u origen

4. DoS(Denegacion de Servicio): Un ataque cibernético a una red con el propósito de interrumpir su funcionamiento normal. Consiste en inundar el tráfico del objetivo con el fin de abrumar el sistema

y denegar el tráfico a las peticiones legitimas.