EXAMEN – PARTE 1

1. EL MURAL DE LAS SIETE CLASES

1. Capa Física
Es la encargada de la transmisión de bits a través de medios físicos, definiendo aspectos eléctricos, mecánicos y de procedimiento. Incluye la descripción de cables (par trenzado, coaxial, fibra óptica) y de ondas de radio. También de técnicas de modulación y multiplexación (FDM, TDM, WDM).

2. Capa de Enlace de Datos
Permite el intercambio fiable de tramas entre dos nodos, que se encuentren conectados. Se encarga de la detección y corrección de errores (CRC, códigos Hamming), el control de flujo para evitar saturaciones y el encapsulado de los paquetes de la capa de red. Por último emplea protocolos como ventana deslizante o parada y espera.

3. Capa de Red
Su función principal es determinar cómo encaminar los paquetes desde el emisor hasta el receptor, a menudo atravesando varios routers intermedios. Su cometido incluye la elección de la ruta (algoritmos de enrutamiento), la gestión de direcciones lógicas (por ejemplo, IP) y el control de la congestión a nivel global.

4. Capa de Transporte
Ofrece un servicio de transporte extremo a extremo. Dos ejemplos habituales son UDP (sin conexión ni control de congestión) y TCP (orientado a conexión, con control de flujo y congestión, además de gestión de reordenación de segmentos). Aquí aparecen también los conceptos de puertos y sockets.

5. Capa de Sesión
No se detalla en los apuntes, pero se encarga de establecer, mantener y sincronizar "sesiones" o diálogos entre aplicaciones en distintos sistemas. Administra puntos de control para recuperación y define cómo se gestiona el intercambio continuo de información.

6. Capa de Presentación
Tampoco figura de manera específica en los materiales. Su función principal es adaptar los datos para que distintas aplicaciones los interpreten de forma coherente. Facilita la conversión de formatos (p. ej., ASCII a EBCDIC), además de la compresión y el cifrado, si resulta necesario.

7. Capa de Aplicación
Se relaciona con los protocolos y servicios empleados directamente por los usuarios, como DNS, correo electrónico (SMTP, POP3, IMAP), HTTP o FTP. Aporta herramientas para la resolución de nombres, envío y recepción de mensajes, descarga y carga de archivos, y navegación web.

En la actualidad, la mayoría de los sistemas funcionan con el conjunto de protocolos conocido como **TCP/IP**, una versión más compacta y práctica del modelo de referencia OSI. Se suele explicar dividiéndolo en cuatro capas:

1. **Acceso a la Red**
   Integra buena parte de lo que en el modelo OSI serían las capas Física y de Enlace de Datos. Su objetivo principal es mover bits o tramas entre dispositivos a través de un medio físico ya sea alámbrico o inalámbrico. Es la encargada de realizar tareas como detección y corrección de errores o manejar direcciones físicas (MAC).

2. **Internet**
   Se encarga de la entrega de paquetes a lo largo de toda la red, asignando direcciones IP a cada dispositivo y dirigiendo los paquetes por las rutas más adecuadas (encaminamiento). De esta forma, un mensaje puede atravesar múltiples redes y routers hasta llegar a su destino.

3. **Transporte**
   Garantiza la comunicación extremo - extremo. Aquí encontramos dos protocolos clave:

   - **TCP**: ofrece un canal fiable (control de flujo, verificación y reordenamiento de segmentos).
   - **UDP**: más sencillo puesto que no establece conexión, lo que lo hace rápido y eficaz para aplicaciones en tiempo real o que toleran pérdidas.

4. **Aplicación**
   Incluye los servicios más visibles para el usuario, como el web (HTTP), el correo (SMTP, POP3, IMAP) o la transferencia de archivos (FTP). Cada uno de estos servicios usan puertos específicos para que distintas aplicaciones puedan funcionar simultáneamente en un mismo dispositivo.

En la práctica, los datos “bajan” por estas capas desde la aplicación del emisor (que los encapsula) hasta la capa de Acceso a la Red (que los transmite), y, al llegar al receptor, se hace el proceso inverso (desencapsulación) para que los datos terminen en la aplicación de destino.

2. LOS DOS PERGAMINOS DEL MENSAJERO

TCP (Transmission Control Protocol)

1. **Orientado a conexión**: Antes de enviar la información, se realiza un intercambio previo de mensajes (el proceso de "three-way handshake") entre emisor y receptor.
2. **Fiabilidad**: TCP se asegura de que todos los datos lleguen, confirmando su recepción. Si algo se pierde, se transmite de nuevo. Ordena los datos en caso de que lleguen desordenados.
3. **Control de flujo y congestión**: Controla la velocidad de envío según la capacidad del receptor y la situación de la red, para no sobresaturarla

Ventajas

- **Transmisión confiable**: asegura que los datos lleguen completos y ordenados.
- **Evita la pérdida excesiva**: su sistema de reintentos y ajustes de ventana disminuye la probabilidad de que se produzca una pérdida de paquetes.
- **Adecuado para aplicaciones que no toleran errores**: envío de archivos, navegación web o correo electrónico.

Desventajas

- **Mayor sobrecarga**: La conexión y la confirmación de paquetes generan retraso adicional.
- **Complejidad**: requiere una gestión más elaborada de ventanas, temporizadores y confirmaciones de recepción.
- **Menor rendimiento en tiempo real**: si la aplicación demanda inmediatez y puede tolerar pérdidas, TCP puede ser demasiado estricto y lento.

UDP (User Datagram Protocol)

1. **No orientado a conexión**: Envía datagramas sin necesidad de establecer ningún tipo de acuerdo previo, lo que reduce los tiempos de arranque.
2. **Baja sobrecarga**: Apenas tiene cabecera (8 bytes) y no envía confirmaciones de recepción.
3. **Sin control de congestión**: No regula la velocidad según la red, así que puede ocasionar pérdidas si se satura el canal.

Ventajas

- **Baja latencia:** los datos se envían sin esperas adicionales, ideal para aplicaciones en tiempo real (voz sobre IP, videoconferencias, streaming).

- **Simplicidad**: Consume menos recursos que TCP y resulta fácil de implementar.
- **Flexibilidad**: funciona bien para servicios que implementan su propio control de errores en niveles superiores (por ejemplo, DNS).

Desventajas

- **No garantiza entrega ni orden:** los paquetes pueden perderse o llegar desordenados sin que exista una corrección automática.
- **No gestiona congestión**: Si la red se sobrecarga, el protocolo no hace nada por remediarlo.

Conclusión

TCP encaja a la perfección en situaciones donde es crucial que cada byte llegue intacto y en el orden correcto (como descargar un fichero, usar una aplicación de correo o navegar por la web).

UDP funciona mejor cuando la prioridad es la inmediatez y se puede tolerar cierto grado de pérdida (como en streaming de vídeo o llamadas de voz), o cuando la aplicación ya maneja sus propios controles de error (caso de DNS).

3. ENIGMA DE LAS SUBREDES

1. Máscara resultante

- **Máscara original (Clase C)**: /24 → 255.255.255.0
- **Se requieren 4 subredes** → Se necesitan 2 bits de subnetting (porque 2^2 = 4).
- **Nueva máscara**: /24 + 2 = **/26**
- En notación decimal punteada: **255.255.255.192**

2. Rango de direcciones en cada subred

Con **/26**, se tienen **6 bits** para la parte de host (32 - 26 = 6). Por lo tanto:

- **Cantidad total de direcciones** en cada subred: 2^6 = 64
- **Direcciones utilizables para hosts** en cada subred: 64 - 2 = 62
  (se restan la dirección de red y la de broadcast)

3. Resumen

1. **Máscara de subred**: /26 (255.255.255.192)
2. **Hosts utilizables por subred**: 62
3. **Explicación breve**:
    - Se parte de un /24 (clase C).
    - Para dividir en 4 subredes, se necesitan 2 bits de subnetting (2^2=4).
    - De /24 se pasa a /26, quedando 6 bits para hosts (2^6=64 direcciones totales, 62 utilizables en cada subred).

4. LA ENCRUCIJADA DE LAS RUTAS

El tótem con flechas representa un router equipado con una tabla de enrutamiento. El dispositivo (router) se encarga de decidir la ruta que deben seguir los paquetes de datos para llegar a su destino dentro de una red o entre redes

Una tabla de enrutamiento es una base de datos interna que utilizan los routers para tomar decisiones de encaminamiento. Cada tabla indica:

- La red del destino
- La máscara de subred
- El siguiente salto
- Una métrica que ayuda a elegir el mejor camino

Cuando un paquete llega al router, el router consulta su tabla de enrutamiento, buscando la mejor coincidencia con la dirección de destino del paquete y lo reenvía por el camino correspondiente

Flechas talladas en piedra – Enrutamiento estático:

- Las rutas son preconfiguradas manualmente por el administrador
- No cambian aunque la red falle o cambie
- Proporcionan más control, consumen menos recursos, pero no se adaptan a fallos ni cambios

Flechas móviles – Enrutamiento dinámico:

- Las rutas se calculan automáticamente con protocolos como RIP, OSPF o BGP
- Se actualizan automáticamente al detectar cambios en la red
- Tiene mayor resiliencia y automatización, pero supone un mayor uso de CPU y tráfico de control

5. EL GUARDIÁN DE LA MÁSCARA ÚNICA

La técnica moderna del guardián es NAT (Network Address Translation), un mecanismo que permite que múltiples dispositivos dentro de una red privada puedan acceder a Internet usando una única dirección IP pública. El router actúa como el guardián puesto que:

- Cambia la dirección IP privada del emisor por la IP pública
- Mantiene una tabla para recordar qué puerto interno hizo la solicitud
- Cuando llega la respuesta, la redirige correctamente al dispositivo que la originó

Los beneficios que NAT en las redes actuales son:

- Ahorro de direcciones IP públicas: Se pueden conectar toda una red privada a Internet con solo una dirección IP pública
- Seguridad adicional: Oculta las direcciones internas de la red, dificultando accesos no autorizados desde el exterior

DOCUMENTACIÓN - EJERCICIO 1 PRÁCTICA

El ejercicio se divide en 2 ciudades, formadas por la topología física básica cada una de ellas. La topología física básica consiste en:

- 1 Router (modelo 1941)
- 1 Switch (modelo 2960)
- 3 PCs

Cada ciudad tiene una red local LAN propia.

Los dos routers se conectan directamente mediante un enlace serial (Cable Serial DCE/CTE). Este enlace actúa como el puente que une ambos reinos

- Serial (192.168.3.0/24)

Direccionamiento IP

- LAN Router1
  - Red: 192.168.1.0/24
  - IP Router1 (interfaz LAN): 192.168.1.1 255.255.255.0
  - Los PCs del reino1 tienen IPs en el rango 192.168.1.x
- LAN Router 2
  - Red: 192.168.2.0/24
  - IP Router2 (interfaz LAN): 192.168.2.1 255.255.255.0
  - Los PCs del reino2 tienen IPs en el rango 192.168.2.x
- Enlace Serial (entre Router1 y Router2)
  - Red: 192.168.3.0/24
  - IP Router1 (Serial): 192.168.3.1 255.255.255.0
  - IP Router2 (Serial): 192.168.3.2 255.255.255.0
  - El Router2 (el DCE) configura clock rate en la interfaz serial (128000)

Para que cada Router conozca la red del otro, se configuran rutas estáticas apuntando al próximo salto sobre el enlace serial:

- En Router1: ip route 192.168.2.0 255.255.255.0 192.168.3.2
- En Router2: ip route 192.168.1.0 255.255.255.0 192.168.3.1

Gracias a esto los PCs de un reino pueden mandar paquetes a dispositivos del otro reino

DOCUMENTACIÓN – EJERCICIO PRÁCTICA 2

La red se compone de:

- Un switch con varios puertos, donde están conectados diferentes dispositivos (PCs) pertenecientes a dos VLAN:
  - VLAN10 (“Arquitectos)
  - VLAN 20 (“Escribas”)
- Un Router central que provee enrutamiento entre las VLAN mediante un único enlace físico hacia el switch, en modo trunk

Se crean las 2 VLAN, conectando los puertos correspondientes a cada una

- VLAN 10 (Fa0/2 y Fa0/4)
- VLAN 20(Fa0/1 y Fa0/3)

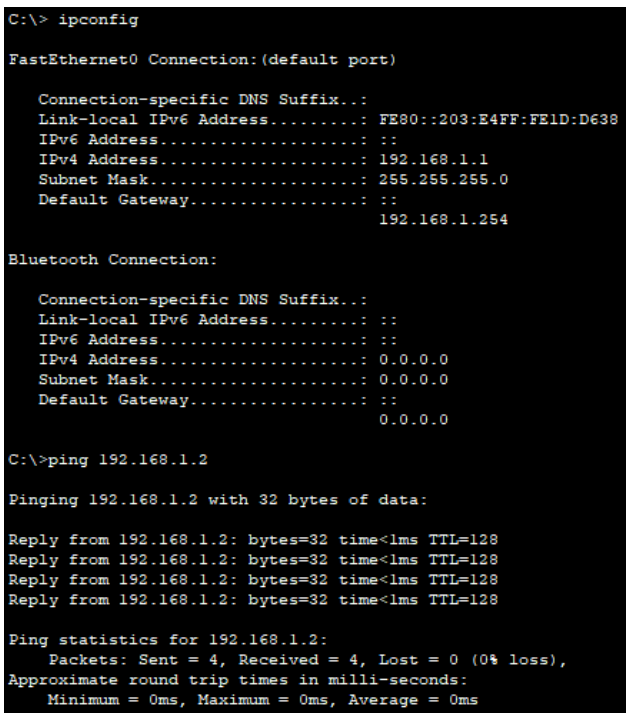
Posteriormente se configuran las subinterfaces para cada VLAN, que hacen posible que un solo enlace físico transporte múltiples VLAN sin necesidad de múltiples interfaces físicas dedicadas

Configuración IP en los PCs

- VLAN 10 (192.168.1.0/24)
  - IP para PC1: 192.168.1.1/24
  - IP para PC3: 192.168.1.2/24
- VLAN 20 (192.168.2.0/24)
  - IP para PC0: 192.168.2.1/24
  - IP para PC2: 192.168.2.2/24

<u>Evidencia de Pruebas:</u>

- ping entre dispositivos de una misma VLAN



- ping entre distintas VLAN

```
C:\>ipconfig

FastEthernet0 Connection:(default port)

   Connection-specific DNS Suffix..:
   Link-local IPv6 Address.....: FE80::203:E4FF:FE1D:D638
   IPv6 Address.....: ::
   IPv4 Address.....: 192.168.1.1
   Subnet Mask.....: 255.255.255.0
   Default Gateway.....: ::
                                 192.168.1.254

Bluetooth Connection:

   Connection-specific DNS Suffix..:
   Link-local IPv6 Address.....: ::
   IPv6 Address.....: ::
   IPv4 Address.....: 0.0.0.0
   Subnet Mask.....: 0.0.0.0
   Default Gateway.....: ::
                                 0.0.0.0

C:\>ping 192.168.2.1

Pinging 192.168.2.1 with 32 bytes of data:

Reply from 192.168.2.1: bytes=32 time<1ms TTL=127
Reply from 192.168.2.1: bytes=32 time<1ms TTL=127
Reply from 192.168.2.1: bytes=32 time=1ms TTL=127
Reply from 192.168.2.1: bytes=32 time=2ms TTL=127

Ping statistics for 192.168.2.1:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 2ms, Average = 0ms
```