RESUMEN COLOQUIO REDES

Introducción a las Redes

REDES → conjunto de recursos de comunicaciones que forman un sistema para transportar información y permitir compartir recursos.

- Clasificación según área geográfica:

	LAN	**WAN**
Definición	Red de área local.	Red de área amplia.
Distancias	Cortas.	Grandes.
Velocidad de Transmisión	Altas.	Bajas.
Calidad de Enlaces	Mayor · Bajo BER.	Menor · Alto BER.
Seguridad	Mayor.	Menor.

PROTOCOLOS → conjunto de reglas y procedimientos que regulan las comunicaciones entre dos o más dispositivos.

- Permiten intercambiar información entre capas que cumplen las mismas funciones.
- Proveen metadata, permitiendo el ensamblado y la segmentación de los bloques de datos.
- Proveen control de flujo, control de errores.
- Brindan servicios que pueden ser **orientados a la conexión (con)** o **no orientados a la conexión (sin)**:

	Servicios con conexión	**Servicios sin conexión**
Monopolio de Recursos	CON y SIN.	SIN.
Orden de Llegada	SÍ.	NO.
Encaminamiento	Un único camino, "como un tubo".	Independiente por cada PDU.
Modo de Operación	Circuito Virtual	Datagrama.

- Proveen modalidad de trabajo en la red para controlar transmisiones en una línea compartida → **sondeo y selección**:
    - Sistemas CON Sondeo y Selección → **ARQ**:
        - Método para: detección de errores, corrección de errores (hacia atrás) y control de flujo.
        - Hace uso de: confirmación positiva [ACK], confirmación negativa [NAK] y *time-outs*.
        - Variantes:
            - **ARQ Stop-and-Wait** → transmisión mensaje a mensaje esperando un ACK o NAK.
                - La operación es *half-duplex* → no requiere comunicación simultánea.
            - **ARQ *Sliding Windows* o Ventanas Deslizantes** → permite al emisor transmitir múltiples segmentos de información antes de comenzar la espera para que el receptor le confirme (con un ACK) la recepción de los segmentos.
                - Concepto de ventana → cantidad de paquetes que puede enviar el transmisor sin esperar recibir conformidad de B.
                - La operación es *full-duplex* → se requiere comunicación simultánea.
    - Sistemas SIN Sondeo – Técnicas de Control de Flujo:
        - Caracteres de control de flujo:
            - **X-ON** → si la estación receptora tiene búfer libre, envía X-ON al otro extremo.
            - **X-OFF** → si la estación receptora tiene búfer saturado, envía X-OFF al otro extremo.
        - Señales de interfaces digitales:
            - **RTS (*Request To Send*)** → el DTE requiere enviar algo al DCE.
            - **CTS (*Clear To Send*)** → el DCE envía un ACK al DTE.

MODELO OSI → modelo genérico de 7 capas o niveles:

#	*Capa*	*Acciones*
7	**Aplicación**	Procesos de red y aplicaciones.
6	**Presentación**	Representación de datos.
5	**Sesión**	Comunicación entre hosts.
4	**Transporte**	Conexiones de extremo a extremo.
3	**Red**	Direccionamiento y mejor ruta.
2	**Enlace de Datos**	Acceso a los medios.
1	**Física**	Transmisión binaria → cables, conectores, velocidades de datos, etc.

- La Capa N: provee servicios a la capa superior y accede a los servicios provistos por la capa inferior.
- El entendimiento entre capas adyacentes dentro de un mismo sistema es entre interfaces.
  El entendimiento entre capas del mismo nivel de distintos sistemas es entre protocolos.

Los enlaces de comunicaciones pueden ser dedicados (el medio no se comparte) o conmutados (el medio sí se comparte).
La conmutación es la forma establecer un camino entre un transmisor y un receptor.

TIPOS DE CONMUTACIÓN → de circuitos o de paquetes:

- **Conmutación de Circuitos** → cada conmutador establece una conexión y, así, queda definido un camino:
  - Hay monopolio de recursos → el recurso de conmutación y el enlace quedarán reservados para la comunicación entre A y B → solamente habrá paquetes de A y B en ese enlace.
  - Es con conexión → se establece una conexión entre A y B, la cual debe ser luego mantenida y liberada.
- **Conmutación de Paquetes** → entre paquete y paquete quedan espacios/tiempos que pueden ser aprovechados por otros paquetes de otras comunicaciones:
  - No hay monopolio de recursos → los recursos de conmutación y los enlaces se comparten.
  - Modos de Operación:
    - **Circuito Virtual** → se establece un único camino (virtual) por el cual viajan todos los paquetes de una misma comunicación → ejemplo: TCP.
    - **Datagrama** → no se establece ningún camino único → cada paquete (que tiene suficiente información para poder enrutarse solo) puede ir por cualquier camino → ejemplos: UDP, IP.

<table>
<tr><th>Conmutación de Circuitos</th><th>Conmutación de Paquetes
(modo Circuito Virtual)</th><th>Conmutación de Paquetes
(modo Datagrama)</th></tr>
<tr><td>Con conexión física.</td><td>Con conexión virtual.</td><td>Sin conexión virtual.</td></tr>
<tr><td>Con monopolio de recursos.</td><td colspan="2">Sin monopolio de recursos.</td></tr>
<tr><td>Ruta dedicada.</td><td>Ruta no dedicada.</td><td>No hay ruta.</td></tr>
<tr><td colspan="2">La ruta se establece para toda la transmisión.</td><td>Cada paquete tiene
su propio encaminamiento.</td></tr>
<tr><td colspan="2">Los datos transmitidos llegan en orden.</td><td>Los datos transmitidos
no llegan en orden.</td></tr>
<tr><td>Transmisión en forma continua.</td><td colspan="2">Transmisión paquetizada.</td></tr>
<tr><td>Puede haber retardo en el establecimiento de la conexión.</td><td colspan="2">Puede haber retardo durante la transmisión de paquetes.</td></tr>
<tr><td>La congestión bloquea el establecimiento de la conexión.</td><td colspan="2">La congestión aumenta el retardo de la transmisión de paquetes.</td></tr>
</table>

Al definir tamaño del paquete en un protocolo, hay que considerar la eficiencia y la tasa de errores (BER):

- Paquetes grandes → más eficientes (hay menos encabezados) → recomendables en canales de bajo BER bajo.
- Paquetes chicos → menos eficientes (hay más encabezados) → recomendables en canales de BER alto.

Redes LAN

- Alcanza las Capas 1 y 2 del Modelo OSI → para el modelo IEEE 802 son: Capa Física y Capas MAC+LLC.
- Subcapa MAC → controla el acceso al medio/canal de difusión, para lo cual hay varios protocolos:
    - ***Contemption* o Contienda o Aleatorio** → los dispositivos pelean entre sí para acceder al medio:
        - Aloha puro → no se sensa la ocupación del canal/medio, el usuario transmite cuando quiere.

          Aloha ranurado → se establecen ranuras de tiempo dentro de cada cual solamente un usuario podrá transmitir
        - CSMA → sensa permanentemente la presencia de la señal portadora: si el medio no está ocupado, lo toma; si está ocupado, espera un determinado tiempo.

          CSMA/CD → sensa la señal portadora y además detecta colisiones.

          CSMA/CA → sensa la señal portadora y además evita colisiones.
    - ***Token Passing* o Paso de Testigo o Determinístico**:
        - Monopoliza el medio/canal mediante el uso de un *token* o testigo de control.
        - El DTE puede transmitir información únicamente si tiene el *token*. Luego de transmitir, se pasa el token para que otro DTE pueda enviar información.
- Dispositivos/Equipos intervinientes:
    - Repetidor/Hub → reciben una señal digital atenuada, la recomponen y la replican en cada puerto.
        - Repetidor → tiene 2 puertos solamente.
        - Hub → tiene N puertos.
    - Bridge/Switch → permiten establecer comunicaciones entre un puerto y otro, usando tablas de direcciones MAC asociadas a cada puerto:
        - Bridge → tiene 2 puertos solamente.
        - Switch → tiene N puertos.
    - Router → enrutan/encaminan paquetes, permitiendo conectar una red LAN con redes WAN.
- VLAN → asociación lógica de estaciones que componen una LAN.

Redes LAN Inalámbricas

- Permiten aumentar el alcance de una red LAN y así poder acceder temporalmente desde dispositivos móviles.

Tecnologías de comunicación inalámbrica

- Infrarrojos.
- ***Spread Spectrum (SS)* o Radio por Espectro Expandido/Ensanchado:**
    - En el transmisor se hace una expansión del espectro, en el receptor se hace una compresión.
    - Provee seguridad en las comunicaciones, reduciendo la detectabilidad.
    - Hay dos técnicas para expandir/ensanchar el espectro:
        - ***Direct Sequence (SS DS)* o Secuencia Directa:**
            - Se expande el espectro y se vuelve al formato original.
        - ***Frequency Hopping (SS FH)* o Salto de Frecuencia:**
            - Es el mismo espectro sólo que "se hace saltar" la frecuencia, lo cual impide al atacante interceptar una comunicación.
- Radio de banda estrecha o Microondas.

Protocolos TCP/IP (LAN)

TCP/IP → conjunto de protocolos (que no están asociados a ningún sistema operativo ni a ningún proveedor) que permiten la interconexión entre redes heterogéneas.

MODELO OSI vs MODELO TCP/IP

Modelo OSI		***Modelo TCP/IP***
Aplicación		Aplicación
Presentación		
Sesión		
Transporte	4	**Transporte**
Red	3	**Internet**
Enlace de Datos	2	**Acceso a la Red**
Física		

PROTOCOLO IP → inunda la red por todos los caminos con el objetivo de llegar a un destino.

- En caso de haber un error, será resuelto por la capa superior.
- Servicio no orientado a la conexión.
- Servicio no confiable → no garantiza que el datagrama llegue a destino.

CONTROL DE ERRORES → IP vs UDP vs TCP

	IP	**UDP**	**TCP**
Detección de Errores	SÍ → en el HEADER. Vía *CheckSum*.	SÍ → en el datagrama UDP y en el pseudoHEADER del Datagrama IP. Vía *CheckSum*.	SÍ → en el Segmento TCP y en el pseudoHEADER del Datagrama IP. Vía *CheckSum*.
Corrección de Errores	NO.	NO.	SÍ → en el Segmento TCP y en el pseudoHEADER del Datagrama IP. Vía ARQ.

UDP vs TCP

	UDP	**TCP**
Tipo de Servicio	Sin conexión.	Con conexión.
Enrutamiento	Un camino independiente por cada PDU.	Todos los PDUs van por el mismo camino.
Entrega de datos	No confiable.	Confiable.
Orden de Llegada	Los datos no llegan en orden.	Los datos sí llegan en orden.
Nombre PDU	Datagrama UDP.	Segmento TCP.
Tamaño PDU	Pequeño.	Grande.
Velocidad	Rápida.	Lento.
Control de Flujo	NO.	SÍ, extremo a extremo (*sliding windows*).
Control de Congestión	-	SÍ, en sistemas intermedios.
Corrección/Detección de Errores	Las aplicaciones que corren sobre UDP requieren corrección/detección de errores.	Las aplicaciones que corren sobre UDP no requieren corrección/detección de errores.
	Ambos realizan direccionamiento, multiplexado y demultiplexado mediante puertos.	
	Ambos residen en la Capa 4 (Transporte) Ambos usan el Protocolo IP como Capa 3 (Internet).	

Protocolos X.25, Frame Relay y ATM (WAN)

X.25 → protocolo para redes WAN de conmutación de paquetes, orientado a la conexión.

- Define una interfaz entre usuario y red, mediante DTE y DCE.
- Si bien está pensado para trabajar con enlaces poco confiables, resuelve esta falta de confiabilidad con detección de errores (Capa 2) y corrección de errores (Capa 3) vía ARQ.
- Capa 1 · Física → define características para poder conectar físicamente un DTE con un DCE.
  Capa 2 · Enlace → define procedimientos para tener un enlace libre de errores.
  Capa 3 · Red → gestiona tanto circuitos virtuales como canales lógicos y maneja la conmutación de paquetes.
- Protocolo HDLC → asegura el enlace de comunicación sin errores; pensado para estructuras jerárquicas.

FRAME RELAY → protocolo para redes WAN de conmutación de paquetes rápida, orientado a la conexión.

- Reemplaza líneas punto a punto dedicadas "LAN to LAN" (donde hay monopolio del recurso utilizado) por líneas conmutadas (donde los recursos se comparten).
- Trabaja sobre enlaces digitales de alta calidad, ideal para transmitir voz y datos a alta velocidad.
- Las conexiones pueden ser permanentes o conmutadas.
- Tiene dos planos de operación:
  - Plano de Control → establecimiento y liberación de conexiones lógicas → trabaja con LAP-D.
  - Plano de Usuario → transferencia de datos de usuarios → trabaja con LAP-F.
    - LAP-F Control → comunicación de extremo a extremo.
    - LAP-F Central/*Core* → comunicación en cada enlace.

ATM → protocolo para redes WAN de conmutación rápida con muy bajos retardos, orientado a la conexión.

- Permite transportar todo tipo de servicios: voz, video, datos y combinaciones entre ellos.
- Requiere capas de adaptación para integrar servicios.
- Reduce funcionalidades en los nodos, delegándolas a los extremos.
- Agrega poca información adicional para el control de errores, confiando en la robustez del medio/canal.
- Para la conmutación, utiliza identificadores de canales virtuales (VCIs) y de trayectos/rutas virtuales (VPIs).
- Capa Fïsica → define interfaces, cables y conectores, así como también velocidades y protocolos.
  Capa ATM → arma/desarma las celdas, hace la conmutación y realiza los controles de congestión y de flujo.
  Capa AAL → segmenta la información de capas superiores y gestiona la señal de reloj.

X.25 vs FRAME RELAY vs ATM

	X.25	***Frame Relay***	**ATM**
Tipo de Servicio	Con conexión.	Con conexión.	Con conexión.
Tipo de Tráfico más adecuado	File Transfer, Batch, Correo electrónico.	Ráfagas (LAN), voz.	Información en tiempo real, voz, video.
Soporte de Comunicaciones	Red analógica y digital. Baja calidad.	ISDN. Mejor calidad.	B-ISDN. Alta calidad.
Nombre PDU	Trama y Paquete.	Cuadro.	Celda.
Longitud PDU	Grande y variable. 16 B / 1024 B.	Grande y variable. 1600 B / 4096 B.	Pequeño y fijo. 53 B.
Velocidad Binaria máx.	64 Kbps.	2 Mbps o más.	622 Mbps ~ 2,4 Gbps.
Control de Errores	Control total. Detección y Corrección salto por salto, capa por capa.	Sólo detección (en todo el cuadro). Capas superiores corrigen.	Sólo detección (en la celda). Capas superiores corrigen.

Protocolo MPLS

- Tecnología que busca mejorar la eficiencia de las redes acelerando el encaminamiento de los paquetes.
- Combina ventajas del control de enrutamiento (Capa 3) y ventajas de una conmutación rápida (Capa 2).

Componentes

- LSRs → routers con capacidad de conmutación de etiquetas.
    - LSR internos → sustituyen etiquetas (sacan una y ponen otra).
    - LSR externos → agregan y sacan etiqueta.
- Etiquetas → identificador corto de longitud fija, la cual es analizada en cada salto.

Funcionamiento

1. Los datagramas IP ingresan al LSR de ingreso, donde se determina el FEC.
    1. Asignado el FEC, se determina el LSR (camino). Y en función del LSR, se aplican las etiquetas.
    2. Ya en la nube, cada datagrama IP tiene una etiqueta.
2. Cuando el datagrama IP llega a un LSR, se cambia la etiqueta… y se van pasando.
3. Cuando el datagrama IP llega al LSR de egreso, éste le saca la etiqueta. Y ahí finaliza el proceso.

Seguridad en Redes

- Confidencialidad o Privacidad → acceso a la información sólo mediante autorización, de forma controlada.
- Autenticidad → asegurarse que la persona sea quien dice ser que es.
- Integridad de datos → modificación de la información sólo mediante autorización; evitar pérdida de datos.

ESTRATEGIAS DE SEGURIDAD → lo mejor es superponer métodos, no limitarse a solamente uno:

- ***Firewall*** → componente que crea una barrera segura entre una red interna/privada y red externa/pública.
    - Provee control de acceso (habilitando o deshabilitando), dando protección frente a ataques externos.
- **Firma digital** → técnica de seguridad aplicada sobre cierta información digital que se intercambia en una red:
    - Basada en criptografía asimétrica (uso de claves - pública y privada- de un usuario) y en función matemática (hash → la salida siempre es de longitud fija).
    - Provee **autenticidad** → el mensaje llegó de parte de quien dice ser que lo envió.
      Provee **integridad** → el mensaje llega sin que se pierda nada en el camino.
      Provee **no repudio** → el transmisor no puede negar que fue enviado por él (su procedencia).
- Capacitación de usuarios y administradores → es importante y necesario que los RRHH estén preparados.
- Red Privada Virtual (VPN) → se logran con enlaces debidamente segurizados, basados en IP Sec.
- **IP Sec** → protocolos de seguridad que permiten agregar encriptado y autenticación a las comunicaciones.
  Tiene dos modos de aplicación:

	Modo Transporte	**Modo Túnel**
Implementación	De host a host, sin que la red intervenga.	Entre gateways.
Dirección IP visible	Se mantienen las direcciones IP originales.	Se usa una nueva dirección IP (la única legible toda la red pública), la cual enmascara la dirección IP original.
Otras Características	Menor protección. Menor procesamiento → más rápido.	Mayor protección. Mayor procesamiento → más lento.