Redes de Información – Prof. Víctor Alsina – Resumen 2019

Concepto de Redes

- Objetivo principal: compartir recursos
- Antes: redes separadas (video, voz, datos, etc).
- Ahora: redes integradas, multimediales (todo por el mismo cable) y convergentes (ej: ISDN). Por la misma red se envía todo tipo de información digitalizada. Ya no hay información analógica

Redes de información

Red: conjunto de recursos de comunicaciones e informática (infocomunicaciones) que forman un sistema para el transporte de información.

Conforme las redes evolucionan, la seguridad se va extendiendo en múltiples ámbitos. Problemas de seguridad aparecen cuando uno se conecta a otras redes.

Concepto de convergencia: convergen todos los tipos de datos en una red única (IP). Voz y datos por la red IP después del año 2000, hasta el 2000 iban por canales separados.

Evolución de las redes

Mainframe (Con terminales bobas) -> Standalone (Computadora Personal) -> LAN (en estos 3 casos se aplica seguridad en ámbito local) -> (token ring) -> WAN -> Internet (en estos 2 ultimos, seguridad en múltiples ámbitos).

Nota: token ring no se usa más. Todo es Ethernet

GPON: Gigabit-capable passive Optical Network

Red óptica pasiva, llegan hasta el corazón de manzana con red óptica y luego distribuyen por cable de cobre (lo hacen las compañías de cable, no las telco)

Fibras ópticas

- FTTN: Fiber To The Network. Es lo que hacen los cableros, llegan hasta el corazón de manzana y luego bajan por cobre a las casas.
- FFTC: Fiber To The Curb. Llegan hasta el cordón de la vereda y luego se distribuyen.
- FTTB: Fiber To The Building. Llegan hasta el edificio y luego dentro del edificio va por cobre.
- FTTH: la fibra óptica llega hasta la casa del abonado. La conexión entre el abonado y el último nodo se puede realizar con una o dos fibras ópticas.

- HFC: Hybrid Fiber Coaxil. Usa las redes CATV (cableros) existentes. Dos partes: desde el abonado hasta el nodo zonal por coaxial + conexión entre nodos zonales por fibra óptica.

Tipos de redes

- Punto a punto: dos o más terminales conectadas de forma directa.
- Difusión multipunto: varias terminales conectadas por una red Ethernet (hub). (LAN Ethernet)
- Conmutada: dos o más terminales conectadas por una nube.
- Internet: varias terminales conectadas con múltiples nubes, que a su vez se conectan entre sí.

Composición de las redes:

Equipos Terminales (DTE): empleados por los usuarios que requieren disponer de esa red.

Nodos de Red: dispositivos que permiten el transporte de información.

Enlaces de Comunicaciones: vinculan equipos terminales con nodos de red.

Clasificación de las redes

- Según el área geográfica
    - Áreas locales (LAN) Local Area Network
    - Áreas extendidas (MAN, WAN) Metropolitan Area Network, Wide Area Network. Hoy por hoy la red MAN se superó por la red WAN. GAN (Global Area Network)

- Según el ámbito
    Públicas: PSDN y PSTN (redes de datos o telefonía de conmutación pública).
    Privadas: RPV (redes privadas virtuales)

- Según el modo de operación
    - Circuitos virtuales (PVC, SVC)
    - Datagramas

- Según la tecnología
    - Analógicas
    - Digitales

- Según el ancho de banda
    - Banda angosta
    - Banda ancha

- Según la parte de la red donde actúa
    - Red de Acceso: interconexión con el usuario, “última milla”.

    - Red de Transporte: interconexión entre centrales (troncales).

Redes por área geográfica

- LAN: área local
- MAN: área metropolitana
- WAN: área amplia o extendida
- GAN: área global

	LAN	WAN
Distancias	Cortas.	Grandes.
Velocidades de transmisión	Alta.	Baja.
Calidad de enlaces	Mayor (bajo BER).	Menor (alto BER).
Uso de canales	... de difusión.	... punto a punto.
Seguridad	Mayor (menos vulnerable).	Menor (más vulnerable).
Afectación por restricciones externas	NO se ven afectadas.	SÍ se ven afectadas.
Infraestructura/Recursos	Infraestructura privada.	Recursos públicos.

Métodos de acceso al medio

- Medios: cobre, aire o fibra.
- Reglas que definen la forma en que un equipo coloca los datos en la red y toma los datos del cable.
- Regulan el flujo del tráfico en la red.
- Los protocolos de acceso al medio definen la forma en la que se producirá la comunicación.
- Pueden ser:
    - **Determinístico**: se organizan las transmisiones.
    - **Contencioso**: todos compiten por entrar al medio.

Paso de testigo (token passing)

- Es una trama especial o testigo que da permiso, o no, de transmisión.
- Se aplica a diferentes redes: token ring, token bus, etc.
- Una terminal de la red puede transmitir en un intervalo de tiempo establecido siempre y cuando tenga el token, si no, no puede transmitir.
- Sirve pare evitar **colisiones**.

La circulación del Token de una máquina a la siguiente se produce a intervalos fijos y en forma de anillo lógico (FDDI). En efecto, si bien IEEE 802.5 emplea un anillo físico, IEEE 802.4 especifica un Bus y ARCnet usa una configuración física en estrella.

CSMA/CD (escucha de portadora y detección de colisión):

- **Portadora**: Señal sin información. Reduce la probabilidad de colisión.
- **Colisión**: 2 estaciones sensan un canal desocupado y transmiten en simultáneo.

Los equipos están escuchando el cable y sólo pueden enviar datos cuando detectan que éste está libre y sin tráfico. Una vez que envían datos, ningún otro equipo puede transmitir hasta que el cable esté libre nuevamente.

Colisión

La estación que ha detectado la colisión procederá a enviar un mensaje jam de 32 bits al resto de estaciones para notificar dicho evento.

Una vez que todas las estaciones han sido notificadas, automáticamente se paran todas las transmisiones y se ejecuta un algoritmo de backoff (o de postergación) que consiste en esperar un tiempo aleatorio (backoff) antes de volver a intentar la transmisión.

Durante los 10 primeros intentos el valor medio del tiempo de espera se duplica mientras que durante los 6 siguientes intentos adicionales, se mantiene. Tras 16 intentos fallidos, el algoritmo notificará un error a las capas superiores.

Al producirse una colisión, los ETD responsables de la misma dejan de transmitir (en realidad se envía una señal de colisión para avisar a todos los ETD de la red de este hecho).

Automáticamente estos equipos generan un número aleatorio entre 0 y 1.

Este número es motivado por el algoritmo de disminución exponencial binaria que propone generar un número aleatorio acorde a la siguiente fórmula:

$$\text{Nro Rand} = 2^n - 1$$

n = cantidad de colisiones detectadas
En la primera colisión: Nro Rand = 2^1-1 = 1 => (Nro Random entre 0 y 1).

Este valor (0 ó 1) establece la cantidad de tiempos de ranura que esperará el ETD para volver a transmitir la trama que ocasionó la colisión, siendo el tiempo de ranura 51,2 µs.

Si los dos ETD generan el mismo valor, colisionarán nuevamente, pero si obtienen valores diferentes, uno de los dos emitirá primero, y cuando pasen los 51,2 µs del segundo ETD y este desee transmitir, encontrará el canal ocupado y no podrá hacerlo (es decir que el primero ganó la compulsa).

Si hubiesen generado el mismo valor, es decir: los 2 ETD = 1 ó los 2 ETD = 0, se producirá la segunda colisión, por lo tanto:

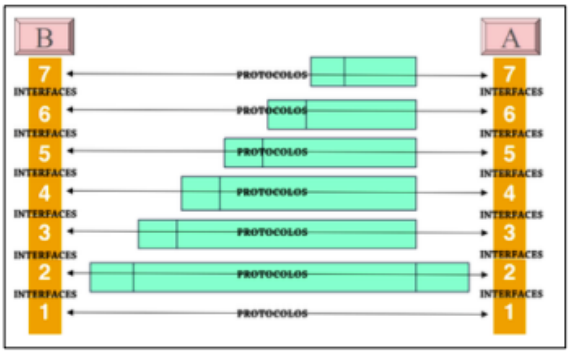
Nro Rand = 2^2 -1 = 3 => (Nro Random entre 0, 1, 2 ó 3)

Resumen:

1. Cuando un dispositivo está muy lejos puede creer que el canal está libre, entonces comienza a transmitir y se produce una colisión.
2. La estación que detecta la colisión envía el mensaje de *jam* al resto de las estaciones para notificarlas.
3. Cuando reciben el *jam*, todas estaciones cesan de transmitir por un tiempo (backoff). Ese tiempo lo mediremos en “tiempos de ranura”.

<u>Protocolos de comunicaciones</u>

- Conjunto de reglas y procedimientos que regulan las comunicaciones entre dos o más dispositivos.
- Permiten intercambiar info entre capas que cumplen las mismas funciones.
- Gobierna el formato y significado de los elementos que se intercambian.
- Permite la **interoperabilidad** entre sistemas



<u>Modelo de referencia OSI</u>

Objetivo: Permitió que los dispositivos de distintos fabricantes se puedan comunicar entre sí.

- Comunicación entre capas iguales -> Protocolos
- Comunicación entre capas adyacentes -> Interfases
- Servicios: provistos por la capa inferior a la superior.
- Entidades: elementos activos de una capa. Provee y usa servicios.

Características:

- Capas separadas para funciones diferentes
- Funciones similares dentro de la misma capa
- Interacción mínima entre capas
- Permite la implementación parcial
- Protocolos entre dos capas iguales, servicios entre capas adyacentes. Una capa brinda servicios a la capa superior y consume servicios de la capa inferior.

- Se ingresa por la capa 7 - Usuario.
- Protocolo de capa par entre cada cada de emisor-receptor (ej; una comprime la otra descomprime)
- Cada capa agrega un header o cabecera de capa (Ej: Cabecera de aplicación). Este header sirve para que el receptor (la misma capa pero del dispositivo receptor) pueda a través de un protocolo en común obtener el mensaje original que tiene datos adicionales para el envío. Ej: Separar un mensaje en paquetes y mandarlo, necesitas agregar info de orden por ejemplo, que el receptor debe sacar para obtener solo el mensaje. Encapsulamiento: Lo que me pasa la capa anterior lo agrego a un header.
  La capa de enlace agrega un trailer para delimitar de los 1 y 0 dónde arranca y termina.

Capas:

Regla nemotécnica: FER Trabaja en un SPA (FERTSPA - Física, Enlace, Red, Transporte, Sesión, Presentación, Aplicación).

Física (1):

- Bits.
- Define la interfaz física entre dispositivos y reglas para la transmisión.
- Determina el código a usar (Manchester, HBN3).
- Determina el medio de comunicación.
- Determina el significado de los 1 y 0 en los dispositivos, amperaje, voltaje.
- No hay control de errores. (No se puede saber si 1 o 0 esta bien)
- **EJ**: ISDN, LAN.

Enlace (2):

- Bits.
- Brindar un enlace seguro y proveer mecanismos para activar, mantener y desactivar el enlace.
- Delimitar tramas. Determinar dónde empieza y termina el mensaje.
  - Eliminar todos los bits auxiliares.
- Garantizar entrega libre de errores utilizando mecanismos de detección y corrección.
  - Recuperar datos perdidos, duplicados o erróneos.
- **EJ**: HDLC, LAP-B.

Red (3):

- Encontrarle un camino al mensaje, el cual tiene origen y destino.
- Permite ir más allá de lo conectado en forma adyacente.
- Funciones de conmutación.

    - Encaminamiento
- Gestiona las prioridades.
- Oculta los detalles de la red subyacente a las capas superiores.
- **EJ**: IP, X25.

Transporte (4):

- Mecanismos para el intercambio de datos de extremo a extremo.
- Control de errores extremo a extremo.
- Proporciona la calidad de servicio solicitada por la capa Sesión.
- Hace una “fragmentación” de los datos que quiere mandar una aplicación, dividiéndolos en paquetes más chicos que puedan ser manejados por las capas de abajo
- **Orientado a la conexión**: Información libre de errores, ordenado y sin pérdidas ni duplicaciones.
- **EJ**: TCP.

Sesión (5):

- Detecta si la comunicación sigue activa o si es necesario reiniciarla en caso de caídas.
- Utiliza mecanismos que se suelen implementar en la capa Aplicación.
- **Control de diálogo**: Solicitud de canales simultáneos (Full Duplex) o alternados (Half Duplex).
- **Recuperación**: Procedimientos de puntos de comprobación para recuperación de fallos e interrupción de operaciones.

Presentación (6):

- Define el formato de los datos que van a intercambiarse.
- Define el formato de compresión para que el receptor pueda descomprimir.
- **Conversión de códigos**: Adaptación de distintos códigos usados en los extremos.
- **Compresión**: De datos.
- **Encriptación**.

Aplicación (7):

- Proporciona a los programas de aplicación un medio para acceder a OSI.
- Toma los datos de usuario y agrega una cabecera de aplicación.
- Incluye funciones de administración general.
    - Mecanismos para implementar sistemas distribuidos.
- **EJ**: Telnet, FTP.

Características de los Protocolos

- **Según Estructura – Arquitectura**
  - **Monolíticos**: único protocolo.
  - **Estructurados**: conjunto de protocolos organizados con una estructura de capas.
- **Según Tipo de Enlace o Red**
  - **Directos**: punto a punto.
  - **Indirectos**: nodos como intermediarios para comunicar.
- **Según Jerarquía**
  - **Simétricos**: entre pares, punto a punto.
  - **Asimétricos**: estructuras jerárquicas, cliente-servidor.
- **Según Normalización**
  - **Normalizados**: se usa siempre el mismo protocolo para cualquier comunicación.
  - **No Normalizados**: un protocolo para cada comunicación.

Servicios

Servicios que brindan los protocolos	**Servicios CON conexión (orientados a la conexión)**	**Servicios SIN conexión (orientados a la no conexión)**
Monopolio de recursos	CON y SIN monopolio de recursos.	SIN monopolio de recursos.
Orden de llegada	CON orden de llegada.	SIN orden de llegada.
Encaminamiento	"Como un tubo" → un único camino.	Encaminamiento independiente por cada PDU.
Transferencia	Transferencia libre de errores.	Enfoque: mejor intento.
Modo de operación	CIRCUITO VIRTUAL.	DATAGRAMA.

Siempre que se trabaje con servicios con conexión (orientados a la conexión) es necesario:
Establecer la comunicación → Mantener la comunicación → Liberar la comunicación.

Tipos de conmutación		**Monopolio de Recursos**	**Conexión**
Conmutación de CIRCUITOS		CON	CON
Conmutación de PAQUETES	***modo CIRCUITO VIRTUAL***	SIN	CON
	modo DATAGRAMA	SIN	SIN

Los enlaces de redes de larga distancia están orientados a la conexión. Mas lento

Los enlaces de área local suelen ser no orientadas a la conexión. Mas rapidos

Funciones de los protocolos

- **Control de flujo** de datos para no saturar con un volumen de info superior al que se puede manejar.
- **Control de la actividad** en el canal de comunicaciones (intervenciones de estaciones)
- **Control de errores** para garantizar que los bloques de datos lleguen sin errores, pérdidas, omisiones o duplicaciones.
- **Segmentación y ensamblado**: armado y desarmado de bloques (PDU).
    - Menor PDU:
        - Control de errores más eficiente
        - Mejor acceso a facilidades de transmisión
        - Menos memoria en buffer
        - Menos necesidad de interrupciones
        - Mas info adicional relativa
        - Mayor tiempo de latencia relativo
    - Mayor PDU:
        - Mayor eficiencia de transmisión
- **Dar transparencia**: asegurarse de no afectar los datos originales con los del protocolo.
- **Encapsulamiento**: agregando info de control a los datos.
- **Sincronismo**: forma de saber que funciona todo ok. Puede ser de carácter o de bloque.
- **Control de la conexión**: establecimiento, transferencia y cierre. Puede incluir manejo de interrupciones y recuperación.
- **Entrega en orden**: uso de numeración secuencial.
- **Direccionamiento**: niveles, alcance, identificadores de conexión y modos (unicast -> a uno solo, multicast -> a un grupo, broadcast -> a todos).
- **Multiplexación**: Varias conexiones en un mismo vínculo. Sondeo y selección.
- **Servicios de transmisión**: prioridad, QOS, seguridad.

Sondeo y selección

- Método para el control de las transmisiones en una línea compartida. Está a cargo del procesador central o estación primaria.
- El server se fija quiénes quieren transmitir y elige a uno para que lo haga.
- Requerimiento automático de repetición (ARQ).
- **Método de control de flujo y control de errores**.

- Requerimiento automático de repetición.

  Sondeo: la estación primaria gobierna el medio compartido entre varias estaciones secundarias. La EP hace un escrutinio, es decir va “sondeando” quien tiene tráfico de las ES. Cuando llega a la ES que tiene el mensaje a enviar, la EP le dice a ES que envíe, y sigue sondeando.
  Selección: la EP que tiene un mensaje previamente enviado por ES, la EP entrega el mensaje (selecciona) al destinatario correspondiente.

- Variantes:
  - Stop and wait (RQ inactiva): es ineficiente si las velocidades son altas y las distancias son grandes. Operacion Half Duplex
  - Sliding Windows (RQ continua): se envían de a varios paquetes (ventana). La ventana se va deslizando y sumando paquetes a medida que se recibe el ACK correspondiente. Si no se recibe el ACK de un paquete en cierto tiempo, éste se reenvía.
  - Tamaño de ventana, eficiencia, necesidad de buffer, confirmación en full duplex (piggyback), requiere nº de secuencia

Protocolo de Ventana Deslizante

- **✓ Capa del nivel de enlace (modelo OSI)**
- **✓ Control de flujo de tipo software**
- **✓ No inundar al receptor con tramas de datos**
- **✓ Proporciona eficiencia en la transmisión**

- Uso de:
  - ACK y NAK.
  - Time out: si no se recibe ACK se empieza a mandar todo el paquete de nuevo.
  - Método para detección de errores.

Sistema SIN Sondeo

X-ON / X-OFF

Son caracteres de control de flujo. Método dentro de banda.

RTS / CTS

Señales de interfases digitales que sirven para control de flujo. Método fuera de banda.

TDMA

Acceso múltiple por división de tiempo.

Sistema con manejo de prioridad

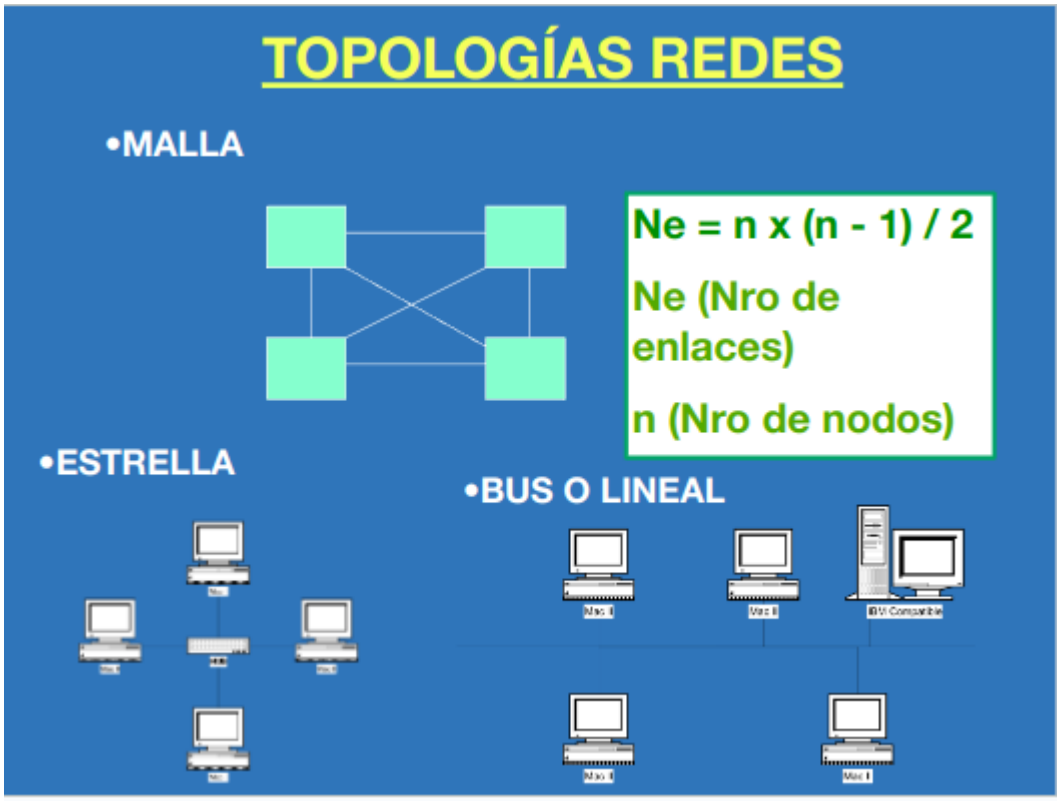
CON PRIORIDAD DE USO DEL CANAL

- ☐ ALOHA RANURADO
- ☐ SENSADO DE PORTADORA
- ☐ PASO DE TESTIGO

SIN PRIORIDAD DE USO DEL CANAL

- ☐ ALOHA ALEATORIO

- ☐ SENSADO DE PORTADORA
- ☐ PASO DE TESTIGO



CUADRO DE CLASIFICACION DE PROTOCOLOS

Primario/Secundario. (Maestro/Esclavo)				*Híbrido*	Igual a Igual							
Con Sondeo y selección		Sin sondeo ni selección			Sin prioridad				Con prioridad			
Parada y espera ▼ BSC	ARQ (Con-tínuo) ▼ SDLC	RTS / CTS Xon / Xoff	TDMA (STDM)	HDLC	TDM	Inserción de registro	Escucha de portadora con colisiones	Paso de testigo sin prioridad	Ranurado con prioridad	Escucha de portadora sin colisiones	Paso de testigo con prioridad	
								En Bus	En Anillo			
				LAP-B	LAP-D		LLC	LAP-X				

Redes LAN

Red LAN se basa en los canales de difusión. Medio está abierto para que operen muchos usuarios (canal de difusión), que es regulado / controlado.

Hay encapsulamiento de los protocolos de las capas de arriba hacia abajo. Cada capa agrega la info de protocolo que corresponde a cada protocolo y capa.

Características

- Peer to peer: todos los miembros de la red son iguales, no hay más ventaja o mayor prioridad.
- **Redes de acceso aleatorio** porque no sabe cuando va a poder emitir.
-Opera con mecanismos de control de acceso al medio (CSMA/CD - Acceso múltiple por detección de portadora con detección de colisiones) → habitación con una mesa y gente que quiere hablar (ejemplo de resumen de final).
- Con los años los estándares de ethernet fueron aumentando (10Mbps, 100Mbps… 10Gb) pero perdura la estructura.
-No pueden emitir más de uno a la vez, se aplica TDMA (transmisión por división de tiempo) en esta primera versión es half-duplex.
-No existe confirmación

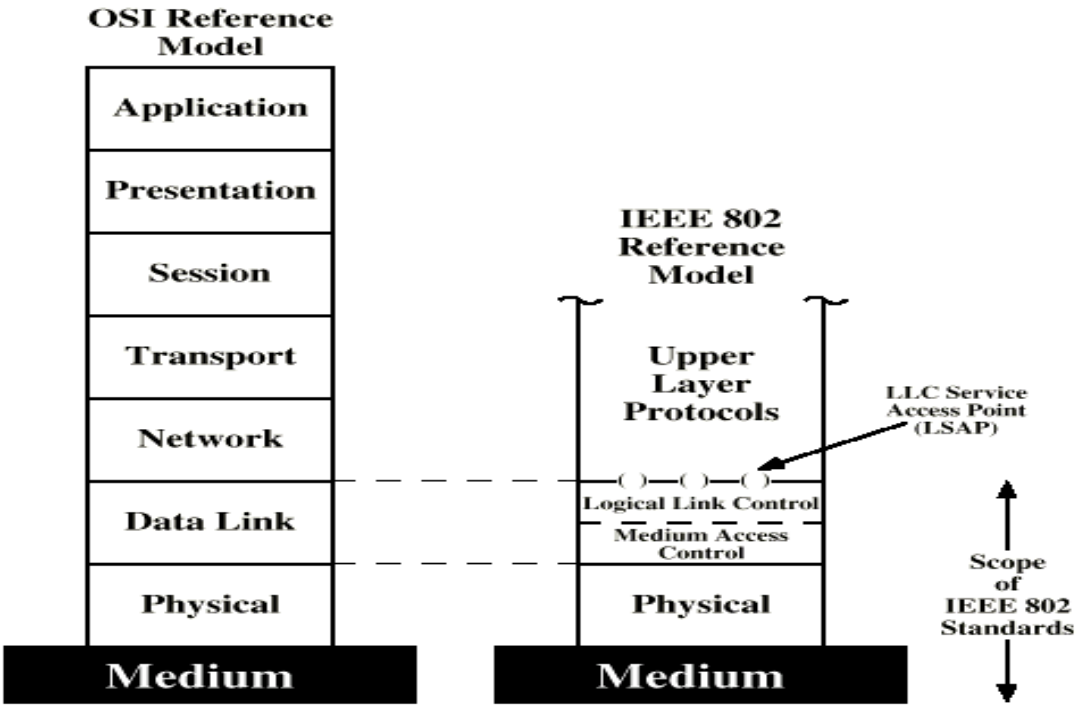
Componentes

- Software: sistema operativo de red (NOS)
- Hardware: medio de comunicaciones, servidores, estaciones de trabajo, placas de red, dispositivos de conectividad (hub, repeater, bridge, switch, router).
- Servidor y cliente.

Clasificación

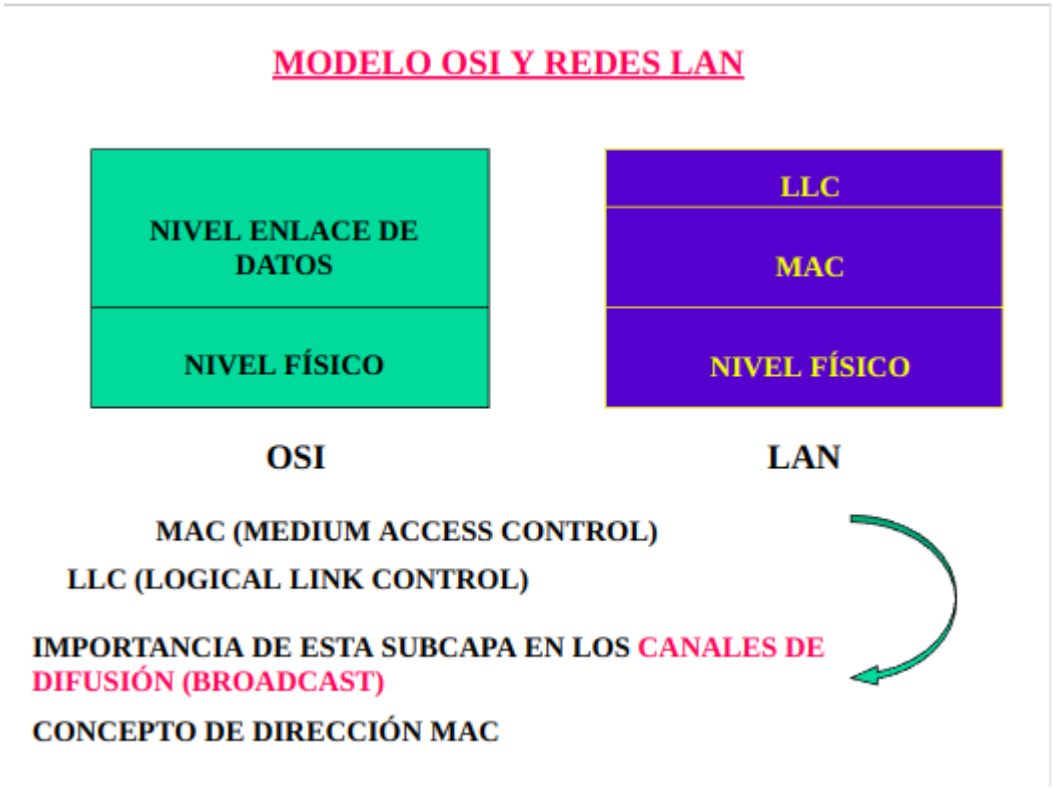
- LAN por cable
- LAN inalámbrica (WLAN)

OSI vs IEEE 802: en el modelo OSI la capa 2 es la Data Link, en cambio en IEEE 802, la capa 2 se divide en LCC (Logical Link Control) y MAC (Medium Access Control).



Protocolos de LAN

- Según la capa que se trate:
  - MAC
  - LCC
- Según el método de acceso al medio:
  - Contention / Token passing
  - Aleatorio / Determinístico
- Según el medio de transmisión y el tipo de red



Dirección MAC

- Dirección de 48 bits asignada a cada tarjeta de red (NIC). La coloca el fabricante.
- Es la dirección física o de hardware, unívoca en cada placa. Identifica el dispositivo.
- Se representa con dígitos hexadecimales. Los primeros 6 identifican al fabricante y los otros 6 son el n° de serie (tarjetas de cada fabricante).
- Dirección de broadcast: FF:FF:FF:FF:FF:FF.

Componentes de la placa de red

- Controlador: formateo de trama, generación de FCS y de clock de tx, codificación, verificación FCS, etc.
- Transceiver: mod/demod, sensado de portadora, detección de colisiones, etc.

Funciones de capa física (capa 1)

- Codificación/decodificación.
- Generación/eliminación de preámbulo.
- Tx y rx de bits.
- Especificación del medio de transmisión y de la topología.
    - Medios de transmisión
        - Par trenzado (UTP, STP)
        - Coaxil (fino, grueso)

        - Fibra óptica
        - Inalámbrico
    - Topologías de LAN
        - Lineal o bus
        - Anillo o ring
        - Estrella o con concentrador (hub/switch)

Ventajas del switch

- Sabe quiénes están conectados.
- Manda la info a quien sabe que la tiene que recibir sin que los demás se enteren, es un conmutador.

Funciones de capa MAC (capa 2)

- Ensamblado (tx) y desensamblado (rx) de tramas.
- Detección de errores (CRC).
- Control de acceso al medio de transmisión.
- La trama MAC tiene encapsulada la PDU LCC dentro suyo.

Técnicas de control de acceso asíncronas (dinámicas) o síncronas (dedicadas en forma fija).

Las asíncronas pueden ser:

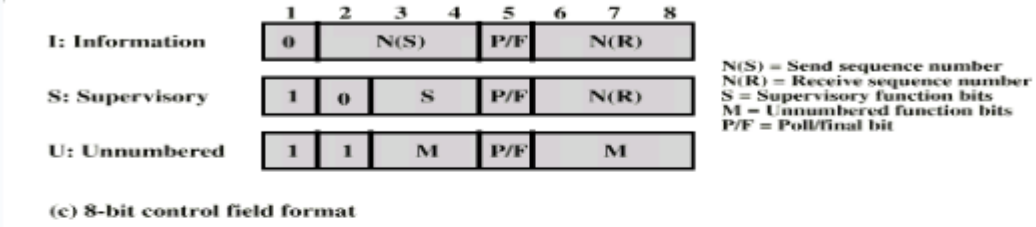
- ☐ Rotación circular. Adecuada cuando muchas estaciones generan tráfico.
- ☐ Reserva. De tiempos para transmitir (ranuras). Adecuada cuando el tráfico es continuo. Poco usada en LAN.
- ☐ Competición. Adecuada cuando el tráfico es por ráfagas.

Funciones de capa LCC (capa 2)

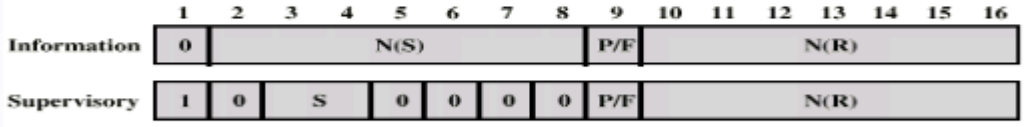
- Interfaz con capas superiores.
- PDU: unidad de datos LCC.
- Opcional: corrección de errores mediante rtx y control de flujo.
- Similares a los protocolos de enlace (HDLC). Se diferencia en:
    - Debe admitir acceso múltiple.
    - La capa MAC libera de algunas funciones de enlace.
- Direccionamiento en LCC: especifica usuarios origen y destino que son protocolos de la capa superior. Servicios que brinda:
    - No orientado a conexión sin confirmación
    - En modo conexión

    - No orientado a conexión con confirmación
- La trama que lleva datos de usuario es la no numerada.

CAMPO DE CONTROL LLC



(c) 8-bit control field format



(d) 16-bit control field format

Es igual al del protocolo HDLC. Usa la versión de 8 o 16 bits según el servicio.

NORMAS LAN IEEE

Sub-capa	CSMA/CD	TOKEN BUS	TOKEN RING	WLAN	PRIORIDAD DE DEMANDA
N SUP	802.1				
N2 LLC	802.2				
N2 MAC	802.3	802.4	802.5	802.11	802.12
N1	COAXIL FINO, GRUESO Y UTP	COAXIL	STP	RADIO WI FI	

CSMA Y ALOHA = ALEATORIO

TOKEN PASSING = DETERMINÍSTICO

LLC: CONTROL DE FLUJO Y GESTIÓN DEL ENLACE

MAC: ENTRAMADO, DETECCIÓN DE ERRORES (CRC) Y ACCESO AL MEDIO

Segmentación:

- **Ventajas**:
  - Aislar el tráfico entre los segmentos.
  - Aumentar el ancho de banda al crear dominios de colisión más pequeños
  - Mejorar la seguridad.
- **Desventajas**:
  - Menor performance ya que se agregan más equipos a la red.
- **¿Como hacerlo?**: Usando un Router, un Bridge o un Switch.

Dominio de colisión

- Es el área de red donde se propagan las colisiones producidas por ocupación del medio en forma simultánea por varios hosts.
- Lo forman todos los dispositivos conectados a un hub. Si hay muchos conectados a un switch NO es DDC, pero cada puerto del switch puede serlo si tiene conectados hubs.
- Los repetidores y hubs propagan colisiones; los puentes, switches y routers, no.
- Cada puerto de switch es un dominio de colisión, pero los puede filtrar

Dominio de broadcast

- Es el área de red donde se propagan las tramas de difusión o broadcast.

- Incluye toda la red y/o las conexiones entre redes.
- Está limitado por routers, es decir, no propagan colisiones

Dispositivos de interconexión de redes LAN

- Hubs
    - No es un conmutador, actúa como repetidor.
    - Capa física.
    - La velocidad de tx de la red se aplica al conjunto.
- Bridge
    - Interconecta dos o más LAN que usan la misma capa física y capa MAC, función similar al repetidor.
    - Almacena y hace control de errores antes de rtx las tramas MAC.
    - Reenvía tramas MAC que corresponden al segmento, no carga a la red.
    - Dispone de memoria, capacidad de direccionamiento y enrutamiento.
    - Conecta redes de distinto tipo.
    - En los más sofisticados, los dispositivos de nivel MAC se conectan vía el control de enlace lógico.
- Switch Ethernet
    - La velocidad de tx de red está aplicada a cada puerto independientemente.

Redes con CSMA/CD: Ethernet 1.0/2.0 vs IEEE 802.3

- Ambos pueden convivir pero la estación que solo use uno no puede comunicarse a través del otro.
- Emplean la misma tecnología de conectividad física.
- Conexión DTE-RED (controladora y transceiver).
- El formato de trama MAC solo difiere en un campo.
- Difieren en que en 2B de la trama Ethernet guarda el tipo de trama y IEEE guarda la longitud. Además Ethernet tiene un indicador de SOF.

Dominio de colisión: algoritmo exponencial binario para tratamiento de colisiones. Sirve para el cálculo del tiempo de espera luego de una colisión.

Tamaño máximo de la PDU = 1518B

64B ≤ Tamaño total de trama ≤ 1518B

8B	6B	6B	2B	46B a 1500B	4B
Preámbulo	**Dirección Origen**	**Dirección Destino**	**Tipo/Longitud de Trama**	**Información (PAYLOAD)**	**Frecuencia de Control de Trama**

En el tamaño total de la trama no se contabiliza al preámbulo porque es de Capa 1.

- *Preámbulo Ethernet II* → `10101010`.
  Preámbulo IEEE 802.3 → `10101011` → el último bit (SFD, Secuencia Diferenciada) es un **1**, se usa para mejorar el sincronismo de bloque.
- Dirección Origen.
- Dirección Destino.
- Ethernet II → Tipo de Trama → qué tipo de información tiene cargada (por capa superior).
  IEEE 802.3 → Longitud de Trama → depende del PAYLOAD, dado que es un campo variable.
- Información (PAYLOAD) → campo de información.
  Si el tamaño de la trama es menor a 46B, se puede agregar un campo de relleno para alcanzar tal valor. Hay que evitar que las tramas sean cortas para evitar tanto $T_{transmisión}$ bajos como $T_{propagación}$ altos, lo cual aumentaría la probabilidad de colisiones.
- FCS - Frecuencia de Control de Trama → CRC-32 → alcanza a todos los campos menos al preámbulo, el cual (al igual que el propio FCS, no se tiene en cuenta para su cálculo).

Ethernet (802.3):

- Sin confirmación.
- **Peer to Peer**: Todos los miembros de la red tienen la misma ventaja.
- **Acceso aleatorio**: No se sabe cuando se va a poder transmitir.
- **CSMA / CD**: Acceso múltiple de portadora con detección de colisiones.
  - Método de acceso al medio.
- **Punto a punto / Multipunto**: Especificar origen y destino.
  - Cuando uno transmite las demás escuchan.
  - Son direcciones MAC.
- **Longitud Trama**: Tamaño mínimo de 64 bytes.
  - Máximo de 1518 sin preámbulo ni SFD.
  - *Es la ventana de colisión para que no colisione con otra estación en caso de mandar un mensaje más corto.*

Trama 802.3 Vs. Ethernet

- **802.3**: Preámbulo (7B) + SFD (1B) + MAC (2B o 6B) + Long. Trama (2B)
- **Ethernet**: Preámbulo (8B) + MAC (6B) + Type (2B)

Tipos de Ethernet básica

- 10B2: coaxil fino
- 10B5: coaxil grueso
- 10Base-T: par trenzado no blindado UTP
- 100Base-TX

- 100Base-T4
- 1000Base-T (UTP Categoria 6 - Actual)
- 10Base-F: fibra óptica

Interfase AUI: es una parte de los estándares IEEE Ethernet que especifica cómo un cable será conectado a una tarjeta Ethernet.

LAN de alta velocidad

- Ethernet conmutada:
    - Usa switch, no se difunde a todos los integrantes del segmento.
    - Cada estación es un dominio de colisión separado. Como no se producen colisiones, no es necesario el algoritmo CSMA/CD.
    - Aprende las direcciones para cada uno de sus puertos.
    - Arma tabla de ruteo.
    - Ventaja sobre el hub: se hace más de una transferencia.
    - No hay necesidad de competir para acceder al medio compartido.
- Gigabit Ethernet: un switch con hubs conectados, que a su vez tienen conectadas terminales.
- 10 Gigabit Ethernet:
    - Incremento del tráfico.
    - Compite con ATM.
    - Uso de fibra óptica, solo modo full dúplex y para distancias de 300m a 40km.
- FDDI: interfaz de datos distribuidos por fibra óptica
- CDDI: interfaz de datos distribuida en cobre

TOKEN PASSING (PASO DE TESTIGO)

REDES QUE USAN ESTE PROTOCOLO DE MAC:

•TOKEN BUS (IEEE 802.4)

•TOKEN RING (IEEE 802.5)

•FDDI (IEEE 802.8)

•CDDI

NO SE PRODUCEN COLISIONES.

USO DEL TESTIGO DE CONTROL (TRAMA PEQUEÑA) QUE CIRCULA CUANDO TODAS LAS ESTACIONES ESTÁN LIBRES.

SE PASA DE UN DTE A OTRO DTE SEGÚN REGLAS.

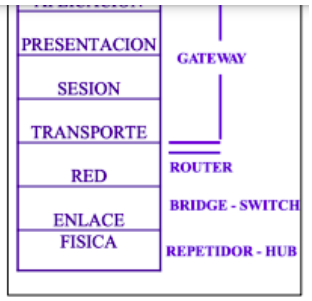
SOLO SE PUEDE TX TRAMA SI SE TIENE EL TESTIGO.

LUEGO DE TX TRAMA SE LIBERA EL TESTIGO PARA QUE OTRO DTE TENGA ACCESO.

SE LE PUEDE ASOCIAR UNA PRIORIDAD AL TESTIGO PARA TX PRIMERO DETERMINADAS TRAMAS.

ANILLO: ACCESO SECUENCIAL , BUS: ACCESO POR DIFUSIÓN

Dispositivos



- **Capa 1 Física - Repetidor – Hub**
  - **Solo recomponen y replican señales. Propagan colisiones y broadcast.**
  - No es un conmutador. Actúa como repetidor.
  - La velocidad de transmisión de la red se aplica al conjunto.
- **Capa 2 Enlace de Datos – Bridge – Switch**
  - **Bridge**
    - **Interconecta dos LAN que usan la misma capa física y capa MAC. Función similar al repetidor.**
    - Alacena y hace control de errores antes de retransmitir las tramas MAC.
    - Reenvía tramas MAC que corresponden al segmento. No carga la red.
    - Dispone de memoria, capacidad de direccionamiento y enrutamiento.
  - **Switch**
    - **Aprenden y almacenan direcciones MAC de los dispositivos alcanzables a través de sus puertos.**
    - Mejora de rendimiento y seguridad.
    - Pasan datos de un segmento a otro liberando la conexión al finalizar.
    - Problema de bucles e inundación.
    - **Clasificación**:
      - **Store and Forward**: alacena información, hace evaluación mediante CRC de errores, evalúa la trama y reenvía. Debo tener buffer suficiente y tiene demora.
      - **Cut Through**: reduce la latencia, lee solo los primeros 6 bytes porque son la dirección destino. No detecto errores porque no leo todo. Variante "libre de fragmento" requiere almacén pero me permite hacer detección de errores.
      - **Adaptive Cut Through**: variante que es compatible con ambos según convenga.
- **Capa 3 – Router**
  - **Tienen capacidad de enrutamiento o encaminamiento de paquetes.**
  - Permiten interconectar redes LAN con redes WAN. No propagan colisiones. Limitan broadcast de MAC pero no broadcast de IP.

Parámetros Características Red

- **Tiempo de Propagación**: se toma el máximo, es el que demanda ir de una estación a otra.
- **Tiempo de Transmisión**: depende del tamaño de la unidad de datos (PDU).

VLAN (LAN Virtual)

- Asociación lógica de estaciones que constituyen una VLAN.
- Se puede definir por puertos, dir MAC, tipo de protocolo o por dir IP.
- Sólo se pueden comunicar a través del router que está conectado a los switch.
- Un dominio de colisión para cada puerto del switch y un dominio de broadcast para todos.
- Cada VLAN es un dominio de broadcast por separado. Si mando un mensaje broadcast le llega a todas, no importa que estén en redes físicas distintas.
- Usado para reducir la difusión en la red al aumentar el número de estaciones
- Estándares:
    - IEEE 802.1Q: múltiples redes pueden compartir un enlace (trunk).
    - IEEE 802.1D: puentes MAC. Incluye el protocolo Spanning Tree (STP). Impide la acción de bucles cuando hay vínculos redundantes.

LAN Inalámbricas (WLAN)

Aplicaciones

- Ampliación de redes: empleos de puntos de acceso (AP) inalámbricos, de celda única o multicelda.
- Interconexión de edificios: empleo de radioenlaces punto a punto que unen routers o bridges.
- Acceso nómade: permite el acceso a una computadora móvil o portátil.
- Trabajo en red ad-hoc: sin servidor central. Peer to peer.

- **Problemas**:
    - Nodo oculto: Una estación cree que el canal está libre pero en realidad está ocupado por un nodo al que no escucha.
        - A → RTS. B→ CTS. C → Capta CTS. A → Envía.

Requisitos

- Rendimiento
- Número de nodos
- Conexión a LAN troncal
- Área de servicio
- Consumo de batería
- Robustez en la transmisión y seguridad
- Funcionamiento de redes adyacentes
- Funcionamiento sin licencia
- Traspaso (Handoff) / Itinerancia (Roaming)
- Configuración dinámica

Tecnologías

- De infrarrojos (IR): haz dirigido, omnidireccional, difusión.
- Radio por espectro expandido:Dos técnicas: Salto de Frecuencia y Secuencia Directa. Banda 900 MHz, 2,4 GHz y 5,8 GHz. topología con concentrador o peer to peer. No necesita licencia ENACOM.
- Radio (microondas) de banda estrecha: son los radioenlaces. Con licencia ENACOM, sin licencia CNC.
- Tipos de espectro expandido:
    - Salto de frecuencia (SF): consiste en modificar la frecuencia sincrónicamente cada cierto tiempo (dwell time).
    - Secuencia directa (SD): consiste en codificar la señal con un código de pseudorruido con el fin de aumentar el ancho de banda y que así se reduzca la densidad de potencia espectral.

	Ejemplo Norma	Banda	Vel máx Alcance	Técnica Met Mod
WPAN Wireless Personal Area Network	**BLUE TOOTH** **IEEE 802.15**	2,4 GHz	1 Mbps a 24 Mbps 10 m	FH GFSK
WLAN	**WI FI Ethernet sin cables** **IEEE 802.11**	2,4 GHz 5,8 GHZ	11 Mbps 54 Mbps 50 m	DS FH
WMAN o WWAN	**WI MAX** **IEEE 802.16**	2,3 a 3,5 GHz	54 Mbps 60 km	
WRAN Wireless Regional Area Network	**IEEE 802.22**	Espacios libres entre 54 a 862 MHz (TV)	23 Mbps 33 km pudiendo llegar a 100 km	OFDMA Sin licencia.

Modelo de capas IEEE 802.11: consta de una capa LLC 802.2, una MAC 802.11 y una compuesta por IR, SF y SD.

Servicios IEEE 802.11

- Asociación / reasociación
- Autenticación y fin de la A.
- Privacidad (WEP – Wired Equivalent Privacy)
- Integración
- Distribución de mensajes

Subcapa MAC 802.11

- Entrega fiable de datos: prevé un protocolo de intercambio de tramas.
    - Mecanismo de 2 tramas: emplea ACK y time out. Repetición de trama si es necesario.
    - Mecanismo de 4 tramas: con esquema previo RTS/CTS que evita colisiones y luego las 2 tramas.
- Control de acceso: protocolo de acceso distribuido o de acceso centralizado.
    - Función de Coordinación Distribuida (DCF): algoritmo de contención para acceso a la totalidad del tráfico. Tipo CSMA (sin detección de colisiones).
    - Función de Coordinación Puntual (PCF): control centralizado opcional. Algoritmo centralizado para acceso libre de contención. Asegura acceso a usuarios.
- Seguridad:
    - Autenticación
    - Privacidad

Formato de trama MAC 802.11

- Control de trama (FC): indica el tipo de trama.
- Duración/Conexión (D/I): indica tiempo de reserva del canal para una tx satisfactoria o identificación de una conexión.
- Direcciones (ADDRESS): depende del contexto. Fuente, destino, estación tx, estación rx.
- Control de secuencia (SC): fragmentación, reensamblado y n° de tramas enviadas.

Tipos de tramas

- Control: sondeo de ahorro de energía, RTS, CTS, ACK, fin periodo libre contención CF, CF-ACK.
- Datos: Datos, +ACK-CF, +CF-POLL, etc.
- Gestión: entre estaciones y puntos de acceso, gestión de asociaciones.

Telefonía móvil

- Elementos:
    - Unidades móviles (teléfonos): contienen una unidad de control, un transreceptor y un sistema de antena.
    - Celdas (radio bases): interfaz entre el MTSO y las unidades móviles. Unidad de control, cabinas de radio, antenas, planta generadora eléctrica y terminales de datos.
    - Conmutador central móvil (MTSO): es el procesador y conmutador de las celdas. Controla el procesamiento y tarificación de llamadas.
    - Conexiones o enlaces: interconectan los tres subsistemas. Antenas de microondas terrestres o líneas arrendadas.
    - Clientes inalámbricos: cualquier computador con una tarjeta adaptadora de red inalámbrica.
    - Portátiles, PDA, equipos de vigilancia, teléfonos inalámbricos de VoIP.
- Técnicas de acceso al medio:
    - FDMA: Acceso múltiple por división de Frecuencias (Las frecuencias que comunican a los usuarios van por distintas frecuencias)
    - TDMA: Acceso múltiple por división de Tiempo (Todas las señales por el mismo medio, empleo de multiplexor y demultiplexor)
    - CDMA: Acceso múltiple por división de Código

- Generaciones del tel. móvil:
    - 1G (analógica),
    - 2G (digitel),
    - 3G (aumento de vel.)
    - 4G
    - 5G.

- Estaciones Base de Telefonía Móvil (En base a lo que quiero cubrir)
    - Microcelda: Corta distancia (Oficina/Entrada de Subte)
    - Macrocelda: Larga distancia (Subte/Shopping)
    - Picocelda

- Planta interna vs planta externa: administra los elementos dentro de la central y el nodo vs administra los elementos fuera de la central o nodo (calle).

Sistemas satelitales

- Sirven para áreas alejadas y de difícil acceso. Hacen posibles comunicaciones donde otros medios no pueden penetrar por su alto costo.
- Algunas frecuencias: V o Q, Ka, Ku (Broadcasting Satelital Service), Ku, C, S, L. (De mas Ghz a menos ghz)
- Tipos de satélites:
    - Geoestacionarios: Proveen comunicaciones fijas para aplicaciones de voz datos y video (bandas C y Ku principalmente). Red Asart. Televisores
    - En órbitas bajas (LEO, MEO): aplicaciones móviles de voz, sensor remoto, sistema de escada, meteorología, ubicación para el GPD. Funciona en banda L

FRECUENCIAS SATELITALES

Banda	Enlace Subida/Bajada	Aplicaciones
V o Q	50/40 GHz	Datos a altas velocidades
Ka	30/20 GHz	Datos y TV a altas velocidades
Ku (BSS)	17/12 GHz	Video directo al hogar
Ku	14/11-12 GHz	VSAT, video e Internet
C	6/4 GHz	Datos, voz y video
S	2/2 GHz	Servicios móviles de voz
L	1.6/1.5 GHz	Servicios móviles de voz

Otros sistemas inalámbricos

- WLL (Wireless Local Loop / Acceso Inalámbrico Fijo): Celdas que conectan varios usuarios de la red pública de la red telefónica conmutada. Usados en sistemas de radio fijos, celulares fijos y de acceso sin alambres. Sustituye el cableado de cobre. No se usa. (Se quiso implementar en Arg). Servicio de voz, fax y módem.

- LMDS (Local Multiplepoint Distribution Service / Servicios Locales Multipunto): Tecnología de banda multiple punto banda amplia. Transporta grandes cantidades de información a muy alta velocidad. Bandas 28,38,40GHz, velocidades 38megas. a distancias cortas (menos de 8km). Sirve para video digital, voz, televisión, acceso a internet. Ejemplo ANTINA
- MMDS (Multichannel Multipoint Distribution Service): Estación base que manda la información en 200MGhz de AB a 2.5Ghz. Usado en televisión restringida inalámbrica. Consiste en un centro de control, un radio transmisor y una antena transmisora + antena receptora, convertidor de frecuencia y receptor decodificador.

- IoT

BANDAS

2.4

mas alcance, mas compatibilidad, menos sensible a los muros o paredes

menor velocidad, mas interferencia y 14 canales

5

mayor vel, menor interf, mas canales (25), no detect por equipos comunes, poco rango de alcance

no detectdo, no geenra interf. afecta masp aredes, mas incompatibolidad

por la longitud de onda. el muro, a la frec. menor lo deja pasar menos que la frecuencia mayor

6ghz (aprovecha ventaja de ambas), aprovecha fortaleza de ambas. mayor alcance y mayor velocidad

Protocolos TCP/IP

- IP -> Capa 3, TCP -> Capa 4.
- Protocolo IP -> direccionamiento con clase y sin clase.

Definiciones

- Internet: conjunto de redes heterogéneas, dispersas e interconectadas vía TCP/IP.
- TCP/IP: conjunto de protocolos que permiten la interconexión entre redes heterogéneas. No están asociados a un sistema operativo ni proveedor.
- Protocolos: proporcionan reglas para la comunicación, sin depender del HW de red.

Comparación entre modelo OSI y modelo TCP/IP

<table>
<tr><th>MODELO OSI</th><th>MODELO TCP/IP</th><th>PROTOCOLOS TCP/IP</th></tr>
<tr><td>Aplicación</td><td rowspan="3">Aplicación</td><td rowspan="3">FTP TELNET SMTP NSP SNMP</td></tr>
<tr><td>Presentación</td></tr>
<tr><td>Sesión</td></tr>
<tr><td>Transporte</td><td>Transporte</td><td>TCP UDP</td></tr>
<tr><td>Red</td><td>Internet</td><td>IP ICMP IGMP</td></tr>
<tr><td>Enlace de datos</td><td>Acceso a la red (incluye parte de la capa de red del OSI)</td><td>ARP
RARP</td></tr>
<tr><td>Física</td><td>Física</td><td></td></tr>
</table>

La capa ARP-RARP sirve para, sabiendo la IP, averiguar la MAC y viceversa.

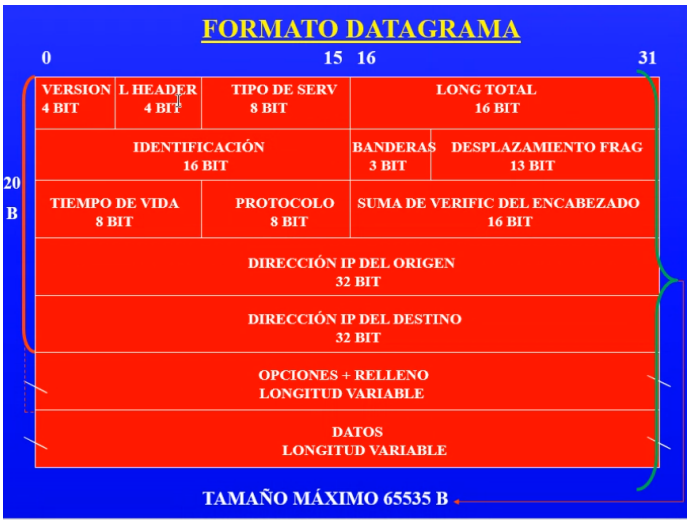
Cliente – Servidor: aplicación distribuida, las tareas se reparten entre los proveadedores de servicios, llamados Servidores, y los demandantes, llamados Clientes. Un Cliente realiza peticiones a otro programa, el Servidor, quien le da respuesta.

Protocolo de internet (IP)

- Define:
    - Unidad básica para la transferencia de datos.
    - Selección de rutas (ruteo).
    - Conjunto de reglas para la entrega de paquetes no confiable.
- Toma los datos del nivel superior (TCP o UDP) y los inserta en internet como datagramas o paquetes.
- Usa ICMP para reportar errores.
- Se basa en servicio no orientado a la conexión y no confiable (sin validación).
- No se garantiza que el datagrama llegue a destino.
- Es un servicio de entrega con el mejor esfuerzo (best effort).
- Los datagramas son independientes, no hay relación entre ellos.
- Los datagramas viajan por distintas redes (Ethernet, FDDI, frame relay, etc).

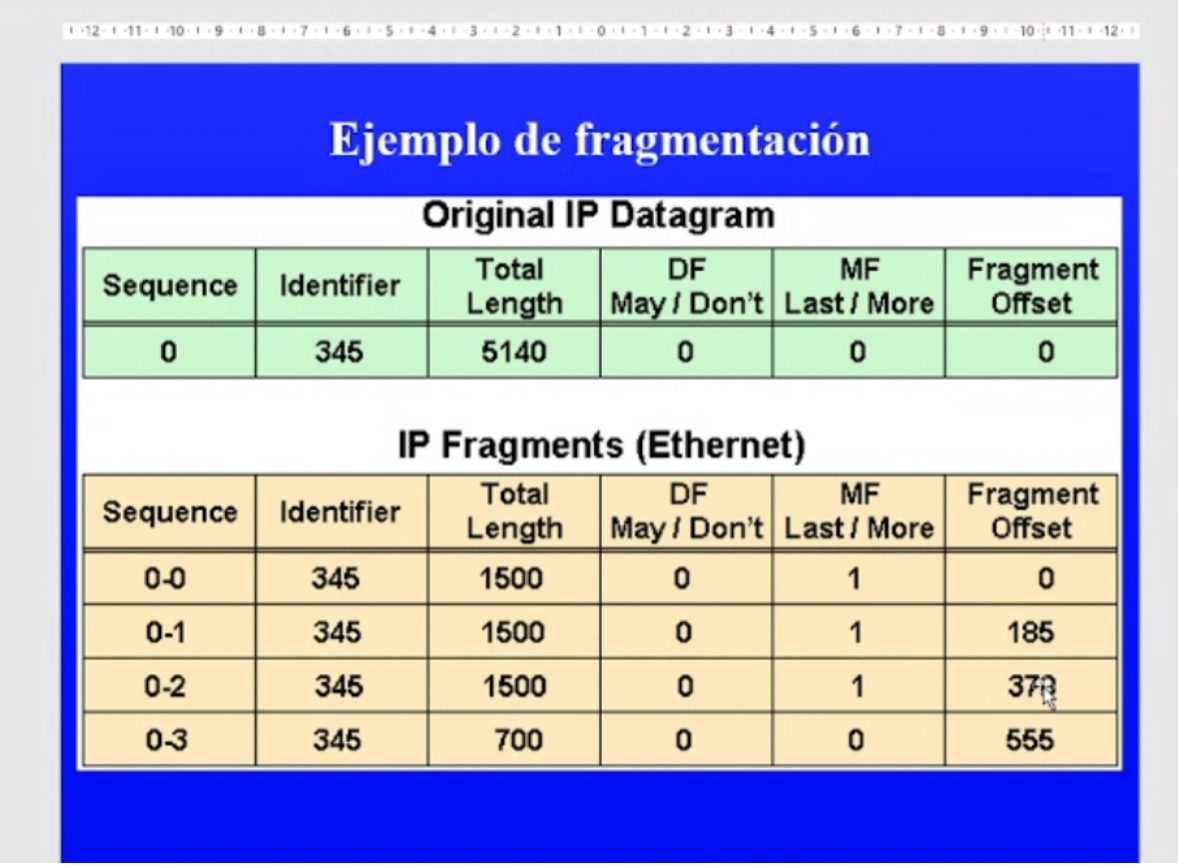
Más sobre datagramas

- MTU: unidad de transferencia máxima de una red. Es el tamaño máximo del campo de datos de la PDU de la red donde se encapsula el datagrama.
- Fragmentación: dividir el datagrama en partes (datagramas más pequeños) que puedan encapsularse en MTU más pequeñas y reensamblarse más tarde. A cargo del router
- Formato datagrama -> Campos:
    - Versión: se verifica la versión del IP (4, 5 o 6).
    - Longitud de encabezado: se miden palabras de 32 bits (máx 16 palabras = 64 B).
    - Tipo de servicio: 6 bits de servicios diferenciados y 2 bits reservados para notificación explícita de congestión.
    - Longitud total: se miden octetos. Incluye encabezado y datos (máx 65535 B).
    - Identificación: identifica al datagrama (fragmentación). Va a servir para cuando se fragmente y se reensamble porque todos los datagramas van a tener la misma identificación.
    - Desplazamiento de fragmento: especifica el desplazamiento en el datagrama original de los datos acarreados en el fragmento (unidades de 8 B).
    - Bandera: controlan la fragmentación dando info (no fragmentar, más fragmentos).
    - Tiempo de vida: tiempo en segundos que el datagrama tiene permitido permanecer en la internet. Luego se elimina.
    - Protocolo: identifica al protocolo de la capa superior (TCP o UDP).
    - Suma de verificación del encabezado: detecta errores.
    - Opciones: no siempre se emplea. Uso para pruebas de red o depuración. Longitud variable.
    - Relleno: asegura que la cabecera tenga una longitud múltiplo de 32 bits.



Fragmentación IP y reemsamblado

- El protocolo IP se usa en una variedad de enlaces de transmisión unidireccionales.
- La mayoría de los enlaces de transmisión imponen un límite más pequeño que la longitud total del datagrama en la longitud máxima del paquete, esa es la MTU.+
- El valor de la MTU depende del tipo de **enlace de transmisión**. Es por eso que el diseño IP permite fragmentar los datagramas IP. La estación receptora los reensambla.
- Para la fragmentación y reensamblado se usan los campos Source IP, Destination, Identification, Total length y Fragment offset y los indicadores More fragments y Don't fragment.



Ejemplo de fragmentación

Original IP Datagram

Sequence	Identifier	Total Length	DF May / Don't	MF Last / More	Fragment Offset
0	345	5140	0	0	0

IP Fragments (Ethernet)

Sequence	Identifier	Total Length	DF May / Don't	MF Last / More	Fragment Offset
0-0	345	1500	0	1	0
0-1	345	1500	0	1	185
0-2	345	1500	0	1	370
0-3	345	700	0	0	555

Direcciones IP

- Para internet son administradas por el NIC.
- Se representan en binario o con 4 números en decimal separados por puntos.
- Se componen de identificador de clase, n° de red y n° de host.
- La dirección IP de cada red debe ser única y la de cada host debe ser única dentro de cada red.
- Una dirección identifica más precisamente a una conexión de red.
- Si un host se mueve de una red a otra, su dirección IP debe cambiar.
- Se emplean para rutear datagramas.
- Un router maneja una tabla de direcciones para enrutamiento. Cada puerto LAN y WAN del router tiene su dirección IP.
- Un host multi-homed es aquel que tiene más de una conexión física. Esto implica una dirección IP por cada una.

Subredes

- Para el mejor aprovechamiento de las grandes redes, se pueden dividir a las mismas en redes más pequeñas.
- Pasos:
    - Determinar cantidad de subredes y cantidad de hosts por subred.
    - Definir máscara de subred, dirección red única para cada subred y rango de direcciones de host válidas.
- VLSM (máscara variable): permite un uso más eficiente asignando distintas máscaras a las interfases de un router.
- CIDR (direccionamiento sin clase):
    - Se asignan bloques de direcciones sin pertenecer a ninguna clase.
    - Uso de máscara en notación CIDR (x.x.x.x/n).
    - Se determinan la primera dirección, la longitud y el broadcast del bloque.
- Técnica de Subred:
    - Permite que una misma dir de red identifique a varias redes físicas.
    - Exige algoritmos modificados de ruteo que contengan tablas con máscaras de subred.
    - Cambia la interpretación de la dir IP. Mayor flexibilidad ya que puede ser independiente en cada red física.
    - Concepto de direccionamiento jerárquico = ruteo jerárquico. Facilita el proceso de ruteo.

Superred: uso de varias direcciones de red para una misma organización (varias clase C). Ruteo: dir IP y n° de conteo (dir contiguas).

Protocolos para resolución de direcciones

ARP	**RARP**
Protocolo de Resolución de Dirección	Protocolo de Resolución de Dirección Inversa
Permite conocer la dirección MAC a través de su dirección IP.	Permite conocer su dirección IP a través de su dirección MAC.
Transmite broadcast MAC con la dir IP destino para que el destino responda con su dir MAC y se registre en la tabla ARP del host.	Transmite broadcast MAC de solicitud para que el servidor RARP dé la dir IP correspondiente a la dir MAC de la máquina solicitante.

Protocolo de control de transmisión (TCP)

- Transferencia confiable y de extremo a extremo.
- Usa IP como nivel 3. Reside en la capa de transporte.
- La PDU se denomina Segmento TCP.
- Realiza multiplexado y demultiplexado de puertos.
- Maneja conexiones full dúplex.

- Usa suma de verificación y n° de secuencia (seguridad y ordenamiento). La suma incluye las dir IP del datagrama, el encabezamiento y los datos del segmento.
- Orientado a la conexión.
- Control de flujo mediante método de ventana deslizante. Divide el flujo de datos en segmentos. Parámetro de tamaño de ventana variable.
- Manejo de time out para rtx. Retrasos variables. (Si no recibe ACK, vuelve a mandar).

Puertos UDP y TCP

- Utilizan números de puerto de protocolo para identificar el destino final.
- Define par (dir IP, puerto) = punto extremo.
- Conexión TCP se identifica por un par de puntos extremos.
- El n° de puerto en una misma máquina puede ser compartido por varias conexiones.

Control de errores

	Protocolo		
Tipo de control de error	IP	UDP	TCP
Detección del Error	Del header	Del datagrama UDP + Dir IP	Del segmento TCP + Dir IP
Corrección / Recuperación	No	No (a cargo de aplicaciones)	Del segmento TCP + Dir IP

TCP:

- **Telnet**: Conexión remota a través de Internet con autenticación.
- **FTP**: Protocolo de transferencia de archivos con autenticación.
- **SMTP**: Simple Mail Transfer. Utiliza ASCII.

UDP:

- **TFTP**: Similar a FTP pero más económico y menos sofisticado.
  - Más rápido y sin autenticación.
- **BOOTP**: Especificar aspectos de arranque como dirección IP o servidor.
  - Mejora el RARP.
- **SNMP**: Simple Network Management
  - Definir la forma y significado de los mensajes.
  - Definir relaciones administrativas entre routers.

IPv6:

- **Campo de dirección**: Pasa de 32 a 128 bits.
    - Espacio de direcciones ampliado.
    - Evita el uso de máscara de IP (NAT).
- Formato de encabezado flexible
- Mecanismo de opciones mejorado.
- Permite características adicionales.
- Provee una funcionalidad para asignación de recursos.
- **Broadcast**: No implementa.
    - Utiliza multicast para enviar un paquete a todas las interfaces de un grupo.

Direcciones:

- Se asignan a interfaces individuales de nodos.
- Permite agrupar por jerarquía de red, proveedores, proximidad, institución, etc.
- Tablas de ruteo más pequeñas.
- Consultas más rápidas.
- 320 bits.
- **Formato**: Notación hexadecimal. 16 bytes con 2 números hexa cada uno.
    - ID Ruteo: 6B.
    - ID Subred: 2B.
    - ID Interfaz: 8B.

—----------

Situación:

- escasez de direcciones IP públicas
- utilizar direcciones privadas en la LAN propia
- usar una única dirección IP pública para el acceso de Internet de todos los equipos de la red local.

En Internet sólo son válidas las direcciones públicas

Para que un dispositivo con una dirección privada pueda acceder a Internet se debe enmascarar su dirección privada con una dirección pública.

Este enmascaramiento de direcciones IP privadas se realiza utilizando el protocolo NAT.

El protocolo NAT, Network Address Translation (Traducción de direcciones de red), hace corresponder un rango de direcciones privadas dentro de una red de área local con una dirección pública de Internet.

NAT (Network Address Traslation)

• Permite usar la red IP con direcciones distintas a las que realmente utiliza.

• Permite convertir espacio de IP no enrutable en direcciones enrutables.

• Permite cambiar de ISP.

- Se desea conectar a Internet, pero no se posee espacio asignado.
- Se puede usar un direccionamiento privado.
- El NAT se configura en Router de borde creando una red interna y una externa (Internet).
- El NAT traduce la dirección interna a una dirección global y única.
- Se necesita cambiar el direccionamiento de IP.

Definiciones de términos

Términos

• Inside local address

– La dirección de IP asignada a un host en la red interna. La dirección es probablemente no legítima.

• Inside global address

– Una dirección de IP legítima que representa una o más inside local IP address para el mundo exterior.

• Outside local address

– La dirección de IP de un host externo como aparenta hacia la red interna.

• Outside global address

– La dirección de IP de un host asignada a este por el propietario del host.

Tipos de NAT

• Traslación Estática

– Establece un mapeo uno-a-uno entre una dirección inside local y una dirección inside global. Es útil cuando un host debe ser accesible desde el exterior mediante una dirección fija.

• Traslación Dinámica

– Establece un mapeo entre las direcciones inside local y un pool de direcciones globales.

MPLS

- Se encuentra entre la capa de Enlace (2) y capa de Red (3)
- Conmutación Datagrama.
- Orientado a la conexión.
- **Funciones**:
    - Control de tráfico (Seguridad)
    - Control de AB
- **Basado en etiquetas**: Identifican las redes destino.
    - Evita meterse en los detalles del mensaje.
- **Ventajas**:
    - Ruteo de IP unicast y anycast.
    - Calidad de servicio adaptable.
    - Reducción de la tarea de conmutación core.
    - Procesamiento a partir de un match exacto de un String de longitud fija.
    - Permite transportar distintos protocolos de capa Red (3

• Incrementar la demanda de throughput

- • Escalamiento

- • Ingeniería de Tráfico

- • Incremento de la funcionalidad del enrutamiento de IP.

• Simplificar la integración de ATM y tecnologías basadas en IP.

- La idea básica es integrar la capa 3 del modelo OSI con la capa 2 (ATM). El beneficio de la rapidez de mover datos en ATM con hardware optimizado y las ventajas de lo protocolos de enrutamiento de IP.

MPLS-Tag Switching

• En L3 convencional, cada vez que un paquete atraviesa una red, cada enrutador extrae la información de forwardeo del encabezado de nivel 3. Este análisis se repite cuantas veces un paquete atraviese hops.

• En MPLS-TS, el encabezado de nivel 3 sólo es analizado una vez. Entonces es mapeado a un pequeño prefijo llamado “etiqueta” (tag-label).

• En cada salto, la decisión de forwardeo es hecha solamente en el valor de la etiqueta. No hay necesidad de reanalizar el encabezado de nivel 3. Debido a que la etiqueta es de tamaño fijo, esto es rápido y simple.

DHCP

- Pertenece a la capa 7
- Centraliza y administra la asignación de direcciones IP.
    - Mantiene un registro de la IP asignada a cada cliente.
- Se encapsula un mensaje en un protocolo de capa Transporte (4) dentro de un datagrama IP cuyo origen y destino se desconoce.
- Protocolo de configuración dinámica de host.
- Del tipo cliente-servidor.
- Extensión del protocolo BOOTP.
- Permite al admin supervisar y distribuir de forma centralizada las dir IP necesarias y, automáticamente, asignar y enviar una nueva IP si el dispositivo es conectado en un lugar diferente de la red.

Metodos:

- ☐ **Asignación manual o estática**
- ☐ Asigna una dirección IP a una máquina determinada. Se suele utilizar cuando se quiere controlar la asignación de dirección IP a cada cliente, y evitar, también, que se conecten clientes no identificados.
- ☐ **Asignación automática**
- ☐ Asigna una dirección IP a una máquina cliente la primera vez que hace la solicitud al servidor DHCP y hasta que el cliente la libera. Se suele utilizar cuando el número de clientes no varía demasiado.
- ☐ **Asignación dinámica**
- ☐ El único método que permite la reutilización dinámica de las direcciones IP. El administrador de la red determina un rango de direcciones IP y cada dispositivo conectado a la red está configurado para solicitar su dirección IP al servidor cuando la tarjeta de interfaz de red se inicializa. El procedimiento usa un concepto muy simple en un intervalo de tiempo controlable. Esto facilita la instalación de nuevas máquinas clientes.

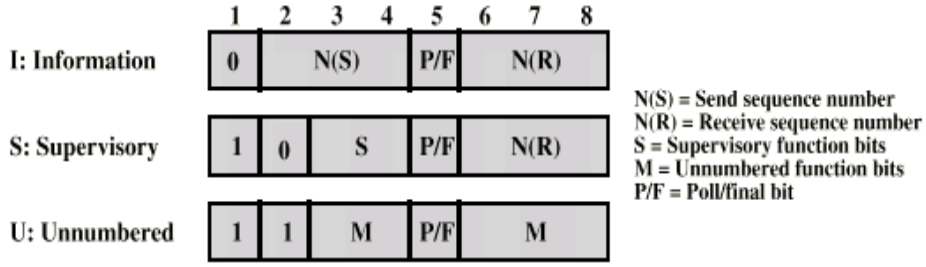
Parametros configurables

- Dirección del servidor DNS
- Nombre DNS
- Puerta de enlace de la dirección IP
- Dirección de Publicación Masiva (broadcast address)
- Máscara de subred
- Tiempo máximo de espera del ARP (Protocolo de Resolución de Direcciones)
- MTU (Unidad de Transferencia Máxima según siglas en inglés) para la interfaz
- Servidores NIS (Servicio de Información de Red)
- Dominios NIS
- Servidores NTP (Protocolo de Tiempo de Red)

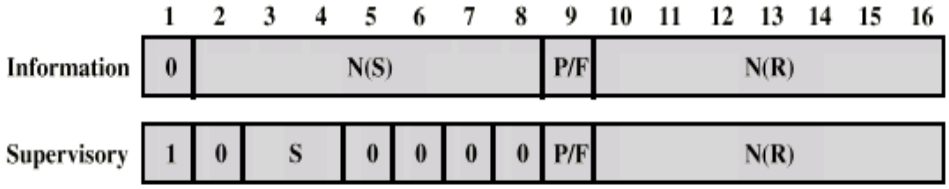
- Servidor SMTP
- Servidor TFTP
- Nombre del servidor de nombres de Windows (WINS)

Protocolo HDLC (High-level Data Link Control)

- Protocolo de capa de Enlace (2)



(c) 8-bit control field format



(d) 16-bit control field format

- Sincrónico, orientado al bit (cambiando un solo bit modifico muchas cosas).
- Permite una transmisión transparente, independiente del código.
- Solo se utiliza en entornos punto a punto.
- **Control de flujo**: ARQ Sliding Windows.
- **Control de errores**: CRC 16
- **Estaciones**:
    - Primarias: Controlan el enlace de datos.
        - Transmiten ordenes y reciben respuestas a secundarias.
    - Secundarias: Responden ordenes.
    - Combinadas: Actúan como primaria y secundaria.
- **Configuraciones**:
    - No equilibrada: Una terminal primaria y varias secundarias.
    - Equilibrada: Todos son combinados.
-
- Con arquitectura de ventana deslizante.

Formato de la trama

- Máx tamaño 1080 bits (135 bytes).
- B: bandera. 8 bits.
- D: dirección. 8 bits.
- C: control. 8 o 16 bits.
- Tres tipos de trama: información (pura), supervisión y no numerada.

Usa relleno de bits

Configuraciones

- Órdenes (estación primaria a secundaria), respuestas (estación secundaria a primaria).
- Balanceada (2P), no balanceada (1P).

Modos de operación

- Respuesta normal (NRM): no bal, se tx solo cuando lo indica la primaria, enlace punto a punto o multipunto, half dúplex.
- Respuesta asíncrona (ARM): no bal, se tx sin permiso de la primaria, enlace punto a punto y dúplex.
- Balanceado asíncrono (ABM): cada estación es primaria y secundaria, enlace punto a punto dúplex.

Tipos de tramas

- No numeradas (U): establecimiento y desconexión. No llevan número de secuencia.
- De información (I): tiene número de secuencia. Empiezan en 0
- De supervisión (S): control de errores y de flujo. Tiene número de secuencia.

Delimitación

- Línea inactiva: 01111111
- Bandera: 01111110

Transparencia

- Inserción/eliminación de bit 0 en secuencia similar a la bandera.
- Bit stuffing: sirve para delimitar la trama. Si 11111, se inserta un 0 en el tx. Si 111110, se elimina el 0 en el rx.

FCS: CRC-16.
Direcciones

- Única para cada secundaria.
- De grupo (enlace multipunto).
- De difusión (enlace multipunto).

Bit P/F (Pool/Final)

- De escrutinio/final.
- Si envía un 1 en la orden, indica que rx debe confirmar.
- Si envía 1 en la rta, indica que rx está confirmando.

Sobre TCP/IP (Importante)

- RFC (Request For Comment): publicaciones que especifican aspectos de TCP/IP.
- PPP (Point to Point Protocol):
    - Permite transferir info desde distintos protocolos y controla el estado de las distintas opciones de enlaces.
    - Realiza encapsulación PPP.
    - Incluye autenticación, compresión, detección de errores y multienlace.
- Socket: es una abstracción como mecanismo de acceso a archivos del sistema operativo. Relaciona aplicación con protocolos TCP/IP sobre detalles del sistema operativo.
- Timestamp: sirve para saber cuándo recibió el mensaje cada destino.

Protocolo ICMP

- Protocolo de mensajes de control de internet.
- Notifica a la fuente sobre errores en la entrega de datagramas para IP.
- Parte de la capa IP.
- Se empaqueta dentro de un datagrama pero no es nivel de transporte.
- Verifica e informa sobre eventos en red IP.
- Mensajes:
    - De eco: verifica la posibilidad de conexión a un nodo (usa comando ping).
    - De respuesta de eco: ídem “de eco”.
    - De redirección: mejoras en ruteo.
    - De tiempo excedido: informa sobre vencimientos de tiempo de vida.
- No corrige problemas de red, solo los informa.
- Como los mensajes de ICMP se transmiten del mismo modo que cualquier paquete, están sujetos a los mismos errores.

Red alcanzable = TCP/IP debidamente configurado en emisor y receptor + puerta de enlace configurada (en caso de redes fuera de la propia) + dispositivos intermediarios configurados con TCP/IP (para el enrutamiento de datagramas).

- **Reporte de error**:
    - Destino inalcanzable: No se puede conmutar o entregar un datagrama por lo que el router envía un mensaje antes de descartarlo.
        - Network Unreachable: No sabe como llegar a la red.
        - Host Unreachable: Llegó a la red pero el host no contesta.
        - Fragmentation Needed: El bit DF = 1 pero se necesita fragmentar.
    - Tiempo de espera agotado: TTL llega a 0 o el host destino dejó de esperar el fragmento.
- **Consulta / Respuesta**:
    - Echo Request / Reply: Saber si la interfaz destino es alcanzable y funciona.
- **Traceroute**: Sirve para conocer la ruta que va a realizar un paquete.
    - Se envía un mensaje a cada nodo del camino con la idea de que se agote en el (Utilizando el TTL.
    - Al agotarse, se descarta y, mediante ICMP, se envía un mensaje del tipo "Tiempo de espera agotado" con la información del nodo.
        - IP, delay, problemas.

Protocolo IGMP

- Protocolo de administración de grupo en internet.
- Es un protocolo de multidifusión que utiliza datagramas para llevar a cabo la comunicación. Intercambia info entre routers.
- Parte de la capa IP.
- Transmite datagramas IP a un conjunto de máquinas (grupo de multidifusión).
- Grupo con proceso dinámico.
- Dirección multidifusión única (clase D). Se usan solo como direcciones de destino.
- Se propaga en una sola red física o a través de varias redes.

Routers

- Dispositivos de nivel 3 del OSI.
- Permiten conectar VLANs. Poseen puertas para enlaces LAN, WAN y para consola.
- Su configuración incluye tablas de ruteo. Aprende direcciones IP.
- Permite la segmentación de una LAN (igual que el bridge y el switch).
- Provee seguridad a la red.
- Tienen interfaces (I/O de paquetes), matriz de conmutación (mover paquetes de entrada a salida) y software (enrutamiento, procesamiento de paquetes, planificación, etc).
- Procesos de paquetes:
    - Aceptarlos por los ports de entrada.
    - Lookup: buscar en la tabla de direccionamiento la dir de destino.
    - Header processing: modifica la cabecera IP (decrementa el TTL y recalcula checksum).
    - Switching: enviar el paquete al puerto correspondiente.
    - Buffering: almacenar el paquete en cola.

- Transmitir el paquete en el port de salida.

Ruteo

- Ocurre en la capa 3
- Es el encaminamiento de los datagramas de una red a la otra mediante rutas.
- Las rutas pueden ser estáticas (ingresadas por el admin de red) o dinámicas (ajustadas automáticamente mediante protocolos de ruteo). La mayoría hoy en día son dinámicas.
- Protocolos de ruteo proveen info sobre accesibilidad, retardos y tablas de ruteo.
- Algunos protocolos de ruteo son: RIP, IGRP, OSPF, EGP.
  - IRP: distribuye info de ruteo dentro de un SA. Info más detallada. (Ej: OSPF)
  - ERP: distribuye info de ruteo entre diferentes SA. Info menos detallada. (Ej: BGP).

- **¿Como se realiza un salto?**: El router hace:
  - Determinar el mejor camino a destino.
  - Conmutar el datagrama: Encapsular en protocolo capa 2.
- **Default gateway**: Camino por defecto para conectarse a otras redes.
- **Default route**: Para paquetes sin información de próximo salto.
  - Hace uso del default gateway
- **Tabla de ruteo:**
  - Almacena la información de la topología y la información que tiene el host de la red.
  - **Columnas**:
    - Red destino
    - Mascara
    - Gateway (próximo salto)
    - Interfaz (Por donde debe ir)
    - Métrica (Cuanto menor sea, más recomendable es ir por ahí)
- **Tipos**:
  - **Estático**: Solo funciona cuando hay un solo camino para llegar.
    - Al definir un camino prioritario, sólo va a intentar ir por ese.
  - **Dinámico**: Utilizado cuando se tienen varias rutas posibles.
    - Intercambio automático de dirección sin intervención.
- **Cálculo del mejor camino**:
  - **Vector distancia**: Menor cantidad de saltos.
  - **Estado del enlace**: Distancias + Delay + Capacidad + Confiabilidad.
  - **Vector camino**. No estima distancia ni costo.

Características:

- **Flexibilidad**: Configurable, adaptable a cambios.
- **Óptimo**: Mejor camino posible dentro de una topología.
- **Rápida convergencia**: Reconfiguración frente a falla de un enlace.
- Robusto.
- Simple.

Protocolos:

- **Interiores (IRP)**: Distribuye información dentro de un AS.
    - Más detalle en la información.
- **Exteriores (ERP)**: Distribuye información entre diferentes AS.
    - Más simple y menos detallado.

BGP:

- Exterior (ERP).
- Border Gateway Protocol.
- Intercambio de información de ruteo entre AS.

OSPF:

- Open Shortest Path First.
- Interior (IRP)
- Calcula una ruta a través de redes suponiendo el menor costo que defina el usuario.
    - Delay o Velocidad de Transmisión.
- Cada Router debe armar un grafo completo de toda la red.

SA (Sistema Autónomo): conjunto de redes o de routers que tienen una única política de enrutamiento y que se ejecuta bajo una administración común, utilizando habitualmente un único IGP (Interior Gateway Protocol). Para el mundo exterior el SA se ve como una única entidad.

Protocolo UDP

- Protocolo de datagrama de usuario.
- **Se encapsula sobre IP**
- Usa IP como nivel 3. Reside en la capa de transporte.
- Estrecha relación entre UDP e IP.
- La PDU se denomina **Datagrama** UDP.
- Transmisiones no confiables, sin validaciones. No implementa control de flujo. Pueden existir pérdidas, duplicaciones, retrasos y entrega sin orden.
- Ventaja: Las aplicaciones deben resolver estos problemas de protocolos.
- **Desventaja: Más veloz que el TCP.**
- Realiza multiplexado y demultiplexado de puertos. Concepto de multiprocesos.
- Orientado a la no conexión (manda y se desentiende del tema).
- Formato (campos):
    - Puerto origen: es opcional. Puede valer 0 si no se utiliza.
    - Longitud: cuenta la cantidad de octetos (encabezado y datos). Valor mínimo es 8 y máximo es 65515.

    - Suma de verificación: es opcional. Si vale 0 no se está usando. Normalmente se usa. Incluye la dir IP origen, dir IP destino (sacadas del datagrama IP), encabezado y los datos del datagrama UDP.

- **Uso**:
    - Procesos simples de Request - Response.
    - Multicast y broadcast.
    - Streaming de audio o video de forma eficiente.
-

Puertos TCP/IP: cuando los datos arriban a su destino, los puertos de TCP/IP definen cuál servicio o propósito tiene dicho tráfico.

Conexiones TCP: son definidas como el par de números (ip_origen : puerto) y (ip_destino : puerto). Conexiones diferentes pueden usar el mismo puerto de destino en el server siempre y cuando los puertos de origen o la IP de origen sean diferentes.

Una conexión TCP es establecida usando un “proceso de 3 vías”:

- Cliente manda la requisición de SYN.
- Server responde con SYN, ACK.
- Cliente manda ACK.

De la misma forma se cierran, solo que en lugar de mandar SYN se manda FIN.

Enrutamiento en TCP/IP

- Enrutamiento: proceso por el cual dos hosts se comunican, usando la mejor trayectoria de una red TCP/IP.
- Componentes del enrutado:
    - Determinar las trayectorias disponibles.
    - Seleccionar la mejor trayectoria.
    - Enviar el paquete por la mejor ruta.
- Principios de enrutamiento:
    - El nodo final necesita saber cómo y cuándo comunicarse con un router.
    - El router necesita saber cómo determinar una ruta adecuada hacia una red remota.
    - El router de la red destino necesita saber cómo conectarse al nodo final.

Uno de los primeros protocolos de enrutamiento fue el Routing Information Protocol (RIP).

RIP evoluciona, el RIPv2, pero no escala a implementaciones de red más extensas.

Para abordar las necesidades de redes más amplias, se desarrollaron dos protocolos de enrutamiento avanzados:

Open Shortest Path First (OSPF)

Intermediate System-to-Intermediate System (IS-IS).

Interior Gateway Routing Protocol (IGRP) y el Enhanced IGRP (EIGRP), (ambos de Cisco) que también escala bien en implementaciones de redes más grandes.

Protocolos de enrutamiento dinámico

- Mantienen tablas de enrutamiento dinámicas por medio de mensajes de actualización del enrutamiento.
- Permiten a los routers compartir info en forma dinámica sobre redes remotas y agregar esta info automáticamente en sus propias tablas de enrutamiento.
- Algunos de ellos son: RIP, IGRP, OSPF, IS-IS, EIGRP, BGP.
- Los protocolos de enrutamiento determinan la mejor ruta a cada red que luego se agrega a la tabla de enrutamiento.
- Ventaja: los routers intercambian info de enrutamiento cuando se produce un cambio de topología. Esto permite a los routers aprender automáticamente sobre nuevas redes y también encontrar rutas alternativas cuando se produce una falla de enlace en la red.
- Propósitos:
    - Descubrimiento de redes remotas.
    - Mantenimiento de info de enrutamiento actualizada.
    - Selección de la mejor ruta hacia las redes de destino y capacidad de encontrar una mejor nueva ruta si la ruta actual deja de estar disponible.

Clasificación de los protocolos de enrutamiento dinámico

RIP: un protocolo de enrutamiento interior por vector de distancia

IGRP: el enrutamiento interior por vector de distancia desarrollado por Cisco (en desuso)

OSPF: un protocolo de enrutamiento interior de estado de enlace

IS-IS: un protocolo de enrutamiento interior de estado de enlace

EIGRP: el protocolo avanzado de enrutamiento interior por vector de distancia desarrollado por Cisco

BGP: un protocolo de enrutamiento exterior de vector de ruta

Protocolos de enrutamiento estático

- Los admin de red crean y producen las rutas.
- Desventaja: en una red muy grande es complicado hacer una por una.

Diferencias entre enrutamiento dinámico y estático

	Dinámico	Estático
Complejidad de la configuración	Suele ser independiente del tamaño de la red	Se incrementa con el tamaño de la red
Conocimientos requeridos del administrador	Avanzado	No requieren conocimientos adicionales
Cambios de topología	Se adapta automáticamente	Se requiere la intervención del administrador
Escalamiento	Adecuado para topologías simples y complejas	Adecuado para topologías simples
Seguridad	Es menos seguro	Es más seguro
Uso de recursos	CPU, memoria y AB de enlace	No se requieren recursos adicionales
Capacidad de predicción	La ruta depende de la topología actual	La ruta hacia el destino es siempre la misma

IGP y EGP

Un SA, o dominio de enrutamiento, es un conjunto de routers que se encuentran bajo una administración en común (ej: la red interna de una empresa o la red de un proveedor de servicios de Internet). Como Internet se basa en el concepto de SA, se requieren dos tipos de protocolos de enrutamiento: protocolos de enrutamiento interior y exterior. Estos son:

Interior Gateway Protocols (IGP): se usan para el enrutamiento de sistemas intrautónomos (el enrutamiento dentro de un sistema autónomo). Se pueden clasificar en:

- Protocolos de enrutamiento por vector distancia: las rutas son publicadas como vectores de distancia y dirección.
- Protocolos de enrutamiento de estado del enlace: crea una topología de la red basándose en info de los demás routers y así encuentra la mejor ruta.

Vector distancia	Estado de enlace
Vista de la topología de la red desde la perspectiva del vecino	Consigue una vista común de toda la topología de la red
Añade vectores de distancias de router a router	Calcula la ruta más corta hasta otros routers
Frecuentes actualizaciones periódicas, convergencia lenta	Actualizaciones activadas por eventos, convergencia rápida
Pasa copias de la tabla de enrutamiento a los routers vecinos	Pasa las actualizaciones de enrutamiento de estado del enlace a los otros routers

Exterior Gateway Protocols (EGP): se usan para el enrutamiento de sistemas interautónomos (el enrutamiento entre sistemas autónomos). BGP es un EGP y es el protocolo de enrutamiento que usa internet.

Protocolos de enrutamiento con clase vs sin clase

Con clase	Sin clase
No envían info de la máscara de subred en las actualizaciones	Envían info de la máscara de subred en las actualizaciones
La máscara se puede inferir de la dirección de red	La máscara no se puede inferir de la dirección de red
No puede usarse en todas las situaciones	La mayoría de las redes lo requieren porque admiten VLSM.

Ahora se suele enrutar sin clase porque permite tener en las subredes máscaras de longitud variable.

Métricas

- Se usan para evaluar y diferenciar entre las rutas disponibles con el fin de seleccionar la mejor.
- Las usan los protocolos de enrutamiento para asignar costos a fin de alcanzar las redes remotas.
- Incluyen:
    - Conteo de saltos: cuenta la cantidad de routers que hay que atravesar. (Usada por RIP).
    - AB: se elige la ruta con el AB más alto. (Usada por IGRP e EIGRP).
    - Carga: considera la utilización de tráfico de un enlace determinado. (Usada por IGRP e EIGRP).
    - Retardo: considera el tiempo que tarda un paquete. (Usada por IGRP e EIGRP).
    - Confiabilidad: evalúa la probabilidad de falla de enlace en base al conteo de errores de la interfaz o las fallas de enlace previas. (Usada por IGRP e EIGRP).
    - Costo: determinado por el IOS o por el admin de red. (Usada por ISIS y OSPF).

Componentes básicos de la arquitectura interna de un router

CPU RAM FLASH NVRAM BUSES ROM INTERFASES

Tipos de servicios:

- **Orientados a la conexión**: Mantiene orden del tráfico.
    - Similar a un tubo.
- **Sin conexión**: Encaminamiento independiente.
    - Puede o no mantener el orden.
    - Similar a una carta.
- **Circuito Virtual**: No decide encantamiento por cada bloque.
    - Establece una ruta de extremo a extremo.
- **Datagrama**: Encaminamiento independiente.
    - No determina rutas de forma anticipada.
    - Más robusto y más adaptable.
    - Implica un mayor trabajo.

Protocolo PPP:

- Punto a punto.
- Capa de Enlace (2)
- Encapsula datagramas IP cuando se envía a través de un Serial.
- Utiliza ARQ Sliding Windows.
- **Funciones**:
    - Transportar datos.
    - Asegurar el enlace y la recepción ordenada.
    - Autenticación.
- **Ventajas**:
    - Permite líneas sincrónicas y asincrónicas.
    - Asignación dinámica de direcciones IP.
    - Transporte de diversos protocolos de red.
    - Permite la creación de VPN cifradas y no cifradas.
- **Desventaja**: No provee cifrado de datos.
- **Etapas**:
    - Establecimiento de conexión: Negociar parámetros.
    - Autenticación: Es opcional a través de:
        - *PAP*: Inseguro porque se envía la información directo.
        - *CHAP*: Se envía la contraseña cifrada.
    - Configuración de red: Negociar parámetros según protocolo de red.
    - Transmisión: Envío y recepción de información.
    - Terminación: En cualquier momento y por cualquier motivo

WAN X25

Características:

- Red de conmutación de paquetes.
- **Transmisión**: Sincrónica.
- **Control de errores**: ARQ Sliding Windows.
- **Orientado a la conexión**: Circuitos virtuales.
- **Ventajas**:
    - Asegura una calidad aceptable cuando el medio no es confiable.
- **Componentes**:
    - Terminal de datos.
    - Red X25: Equipos conmutadores de paquetes.
- **PAD**: Ensamblador de paquetes.

Capas:

- **Física** (1): Define características para la conexión física entre DTE y DCE.
    - X21: Enlace digital. Señal balanceada.
    - X21 bis: Enlace analógico.
- **Enlace** (2): Define procedimientos para un enlace libre de errores.
    - Transmisión full duplex.
    - ARQ Sliding Windows con Piggyback
- **Red** (3): Define formato de paquetes, procedimiento de intercambio para DTE/DCE de VC con los DTE remotos.
    - Circuitos Lógicos (LC): Multiplexar enlace de nivel 2 en canales nivel 3.
    - Circuitos Virtuales (VC): Asociación lógica de múltiples LC entre origen y destino.
    - Modos de operación: Proceso de envío y recepción.
        - *Por paquete*: Sincronismo punto a punto
        - *Caracter*: Sincronismo hasta el PAD y luego asíncrono modo caracter