**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 y convergentes (ej: ISDN). Por la misma red se envía todo tipo de informacion digitalizada.

Concepto de convergencia: convergen todos los tipos de datos en una red única (IP).

Evolución de las redes

Mainframe -> Standalone -> LAN (en estos 3 casos se aplica seguridad en ámbito local) ->

-> WAN -> Internet (en estos 2, seguridad en múltiples ámbitos).

Nota: token ring no se usa más. Todo es Ethernet o 802.5

Redes de información

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

Fibras ópticas

* HFC: Usa las redes CATV existentes. Dos partes: desde el abonado hasta el nodo zonal por coaxial + conexión entre nodos zonales por fibra óptica.
* 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.

Tipos de redes

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

Composición de las redes: enlaces de comunicaciones + nodos de red + equipos terminales.

Clasificación de las redes

* Según el área geográfica
  + Áreas locales (LAN)
  + Áreas extendidas (MAN, WAN)
* Según el ámbito
  + Públicas (PSDN, PSTN)
  + Privadas (RPV)
* 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
  + Red de transporte

Redes por área geográfica

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

| **Diferencias** | |
| --- | --- |
| **Local – LAN** | **Amplia – WAN** |
| Cortas distancias | Grandes distancias |
| Bajo BER | Alto BER (diferencia de 1000) |
| Uso de canales de difusión | Uso de canales punto a punto (EXCEPTO ENLACES SATELITALES DE ACCESO MÚLTIPLE) |
| Uso de la difusión (existen conmutadas) | Uso de la conmutación |
| No restricciones externas | Restricciones externas |
| Infraestructura privada | Recursos públicos |
| Menos vulnerable a la seguridad | Más vulnerable a la seguridad |

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): 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.

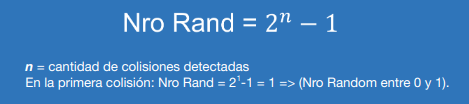
Una vez que todas las estaciones han sido notificadas, automáticamente se paran todas las transmisiones y se ejecuta un algoritmo de backoff (o de postergación) que consiste en esperar un tiempo aleatorio (backoff) antes de volver a intentar la transmisión.

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:



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”.

Protocolos de comunicaciones

* 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**.

Modelo de referencia OSI

* 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.

Clasificación de los protocolos

* Directos o indirectos: según tipo de enlace o red.
* Monolíticos o estructurados: único protocolo vs conjunto de protocolos organizados con una estructura de capas – arquitectura.
* Simétricos o asimétricos: entre pares, primaria-secundaria, cliente-servidor, etc.
* Normalizados o no normalizados: un protocolo y pocas implementaciones vs muchos protocolos y muchas implementaciones.
* Con conexión o sin conexión: según el servicio que brindan.

Servicios

| **Orientados a** | |
| --- | --- |
| **La conexión** | **La no conexión** |
| Con orden de llegada | Sin orden de llegada |
| Como un tubo | Encaminamiento independiente |
| Transferencia libre de errores | Enfoque mejor intento |
| Circuito virtual | Datagrama |
| Envío con confirmación de recepción | Envío sin recepción de feedback |

Funciones de los protocolos

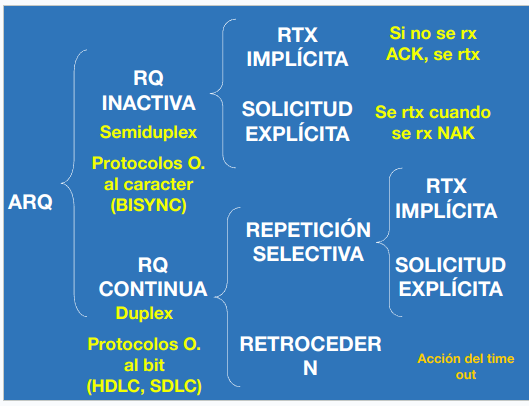
* **Control de flujo** de datos para no saturar con un volumen de info superior al que se puede manejar.
* **Control de la actividad** en el canal de comunicaciones (intervenciones de estaciones)
* **Control de errores** para garantizar que los bloques de datos lleguen sin errores, pérdidas, omisiones 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.
* 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.

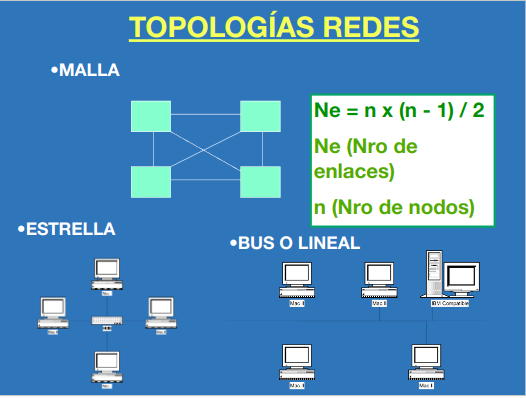
Sistema con manejo de prioridad

**CON PRIORIDAD DE USO DEL CANAL**

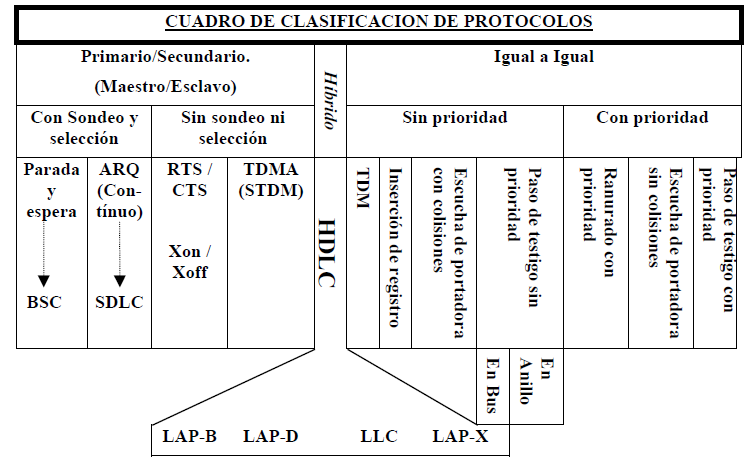
* ALOHA RANURADO
* SENSADO DE PORTADORA
* PASO DE TESTIGO

**SIN PRIORIDAD DE USO DEL CANAL**

* ALOHA ALEATORIO
* SENSADO DE PORTADORA
* PASO DE TESTIGO







**Redes LAN**

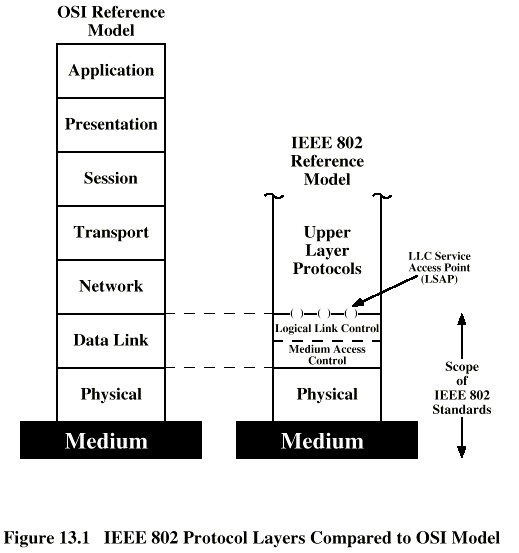
Componentes

* 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

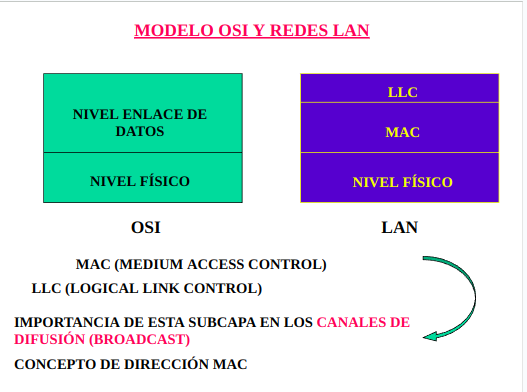
* LAN por cable
* LAN inalámbrica (WLAN)

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 (CDC).
* Control de acceso al medio de transmisión.
* La trama MAC tiene encapsulada la PDU LCC dentro suyo.

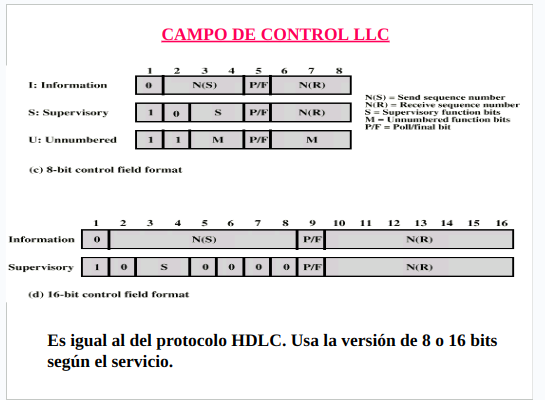
Técnicas de control de acceso asíncronas (dinámicas) o síncronas (dedicadas en forma fija).

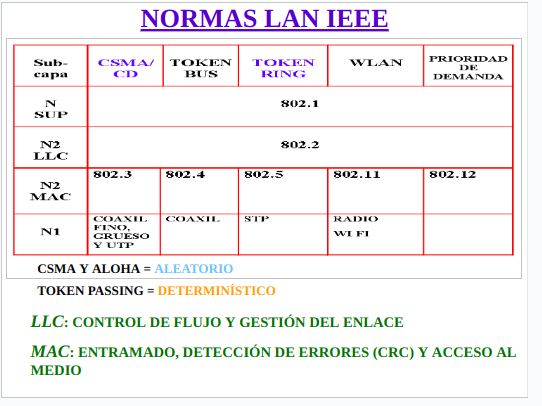
Las asíncronas pueden ser:

* 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.





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.

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.

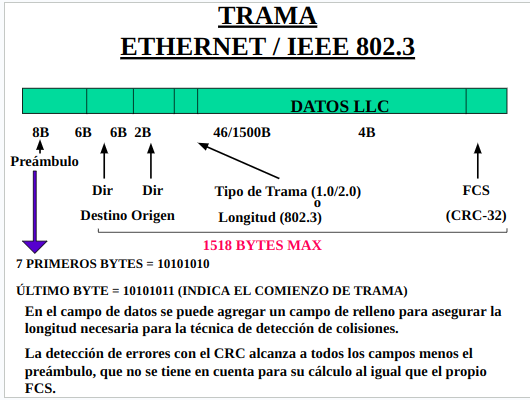
Dispositivos de interconexión de redes LAN

* 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.



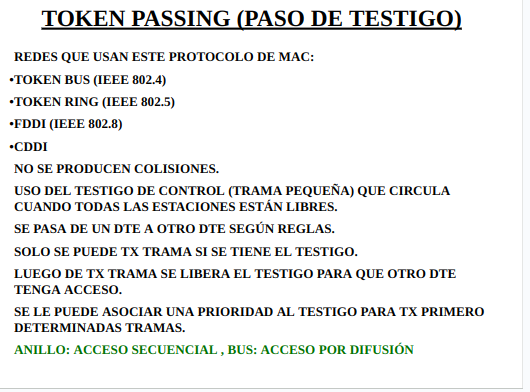
Tipos de Ethernet básica

* 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



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.
* 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.

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: 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.

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): interface 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
  + TDMA: Acceso múltiple por división de Tiempo
  + CDMA: Acceso múltiple por división de Código
* Generaciones del tel. móvil: 1G (analógica), 2G (digital), 3G (aumento de vel.), 4G, 5G.
* Macrocelda vs microcelda: larga distancia (hasta 20 km) vs corta distancia (hasta 1 km).
* 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, Ku (BSS), C, S, L.
* Tipos de satélites: geoestacionarios, en órbitas bajas.

Otros sistemas inalámbricos

* WLL: usados en sistemas de radio fijos, celulares fijos y de acceso sin alambres.
* LMDS: banda amplia. Transporta grandes cantidades de info a muy alta velocidad.
* MMDS: 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.

**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

| **MODELO OSI** | **MODELO TCP/IP** | **PROTOCOLOS TCP/IP** |
| --- | --- | --- |
| Aplicación | Aplicación | FTP TELNET SMTP NSP SNMP |
| Presentación |
| Sesión |
| Transporte | Transporte | TCP UDP |
| Red | Internet | IP ICMP IGMP |
| Enlace de datos | Acceso a la red (incluye parte de la capa de red del OSI) | ARP  RARP |
| Física | Física |  |

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

Cliente – Servidor: aplicación distribuida, las tareas se reparten entre los proveedores 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.
* 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.

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:
  + 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 header | Del datagrama UDP + Dir IP | Del segmento TCP + Dir IP |
| **Corrección / Recuperación** | No | No (a cargo de aplicaciones) | Del segmento TCP + Dir IP |

Aplicaciones

* Telnet – TCP: conexión remota a través de internet. Con autenticación. Nos permite manejar una PC remotamente.
* FTP – TCP: protocolo de transferencia de archivos, copiado de archivos. Con autenticación.
* TFTP – UDP: económico y menos sofisticado que el FTP. Sin autenticación. T=Trivial.
* DNS – UDP: sistema de nombre de dominio. Traduce la dir IP a un nombre significativo de alto nivel. Jerárquico y descentralizado.
* PING – ICMP: envía solicitud de eco, captura la respuesta y realiza estadísticas del estado, velocidad y calidad de la red.
* BOOTP – UDP: protocolo creado para reemplazar el RARP. Especifica aspectos en el arranque, como dir IP máquina, ruteador y servidor.
* DHCP – UDP: protocolo para configuración de host dinámica. Asignación de dir IP por servidor a clientes. Sustituyó al BOOTP.
* SMTP – TCP: protocolo de transferencia de correo simple. Especifica formato de mensajes. Usa el ASCII.
* SNMP – UDP: protocolo de administración de red simple. Definen relaciones administrativas entre routers, forma y significado de mensajes entre otros aspectos.

IPv6

* IP de nueva generación.
* Mejoras:
  + Espacio de direcciones ampliado.
  + Formato de encabezado flexible.
  + Mecanismo de opciones mejorado.
  + Permite características adicionales.
  + Funcionalidad para la asignación de recursos.
* FALTAN DATOS DE ESTE TEMA PERO NO ENTRABA IPv6 EN EL PARCIAL.

Sobre TCP/IP

* 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.

DHCP

* 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.

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).

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

* 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).
* Estrategias:
  + Por vector distancia
  + Por estado de enlace
  + Por vector camino

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.
* 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.
* Las aplicaciones deben resolver estos problemas.
* 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.

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.

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.

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 |
| Frencuentes 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).

HDLC

* Configuraciones:
  + Órdenes / Respuestas
  + Balanceada / No balanceada.
* Modos de operación:
  + Respuesta normal (NRM)
  + Respuesta asíncrona (ARM)
  + Balanceado asíncrono (ABM)
* Tipos de tramas:
  + No numeradas (U)
  + De información (I)
  + De supervisión (S)
* Delimitación:
  + Línea inactiva
  + Bandera
* Transparencia: inserción/eliminación de bit 0 en secuencia silimar a la bandera. Bit stuffing.
* FCS: CRC – 16
* Direcciones:
  + Única para cada secundaria
  + De grupo (enlace multipunto)
  + De difusión (enlace multipunto)
* Bit P/F:
  + De escrutinio/final.
  + Si 1, en orden indica que rx debe confirmar.
  + Si 1, en respuesta indica que rx está confirmado.