UNIDAD N° 1: Arquitectura de las redes de datos.

Clasificación de las redes: LAN, MAN, WAN y GAN. **Redes orientadas y no orientadas a conexión. Clasificación de los protocolos de comunicaciones. Sistemas con sondeo y selección. Sondeo selectivo y de grupo. Sondeo con parada y espera. ARQ continuo (ventanas deslizantes). Sistemas sin sondeo: Xon/Xoff , RTS/CTS y TDMA. Sistemas con manejo de prioridad. Topología de redes LAN y WAN. Ejemplos de arquitectura de redes.**

MECANISMOS DE CONTROL DE TRÁFICO
CONEXIÓN - FLUJO – ERRORES - ACCESO AL MEDIO

- CONTROL DEL TRÁFICO
  - El control del tráfico se realiza mediante la cooperación de varios protocolos.
  - **Protocolo**: conjunto de normas que especifican el intercambio de datos entre elementos de la red.
  - Cada protocolo se ocupa de un aspecto concreto de la comunicación.
    - Ej: Protocolos de enlace de datos, de encaminamiento.

MECANISMOS DE CONTROL DE TRÁFICO
CONEXIÓN - FLUJO – ERRORES - ACCESO AL MEDIO

- Redes Orientadas a Conexión
  - Los elementos de la red que quieran comunicarse han de establecer primero una conexión
  - Una conexión tiene como objetivos, aunque no se pueden garantizar en todos los casos:
    - Los datos lleguen sin errores a su destino.
    - Los datos lleguen en el orden apropiado.
    - No deben producirse problemas de congestión en la red.
  - La red ha de reservar los recursos necesarios para conseguir que se realice la conexión.
    - Ej. Llamada telefónica, protocolo TCP.

MECANISMOS DE CONTROL DE TRÁFICO
CONEXIÓN - FLUJO – ERRORES - ACCESO AL MEDIO

- Redes Orientadas a Conexión
  - Reconocimiento explícito de la conexión
    - La red informa si se pudo o no realizar la conexión
  - Control de errores
    - Se emplean técnicas de detección y corrección de errores
  - Control de flujo y desbordamiento.

  - Ventaja
    - Se preservan mejor los datos del usuario.
  - Desventaja
    - Sobrecarga de trabajo para la red.

MECANISMOS DE CONTROL DE TRÁFICO
CONEXIÓN - FLUJO – ERRORES - ACCESO AL MEDIO

- Redes No Orientadas a Conexión
  - No se establece una conexión
  - No se requiere realizar detección ni corrección de errores
  - No se requiere garantizar que los datos lleguen ordenados
  - No se requiere realizar control de flujo
    - Ej: Comunicación por carta, protocolos UDP e IP.

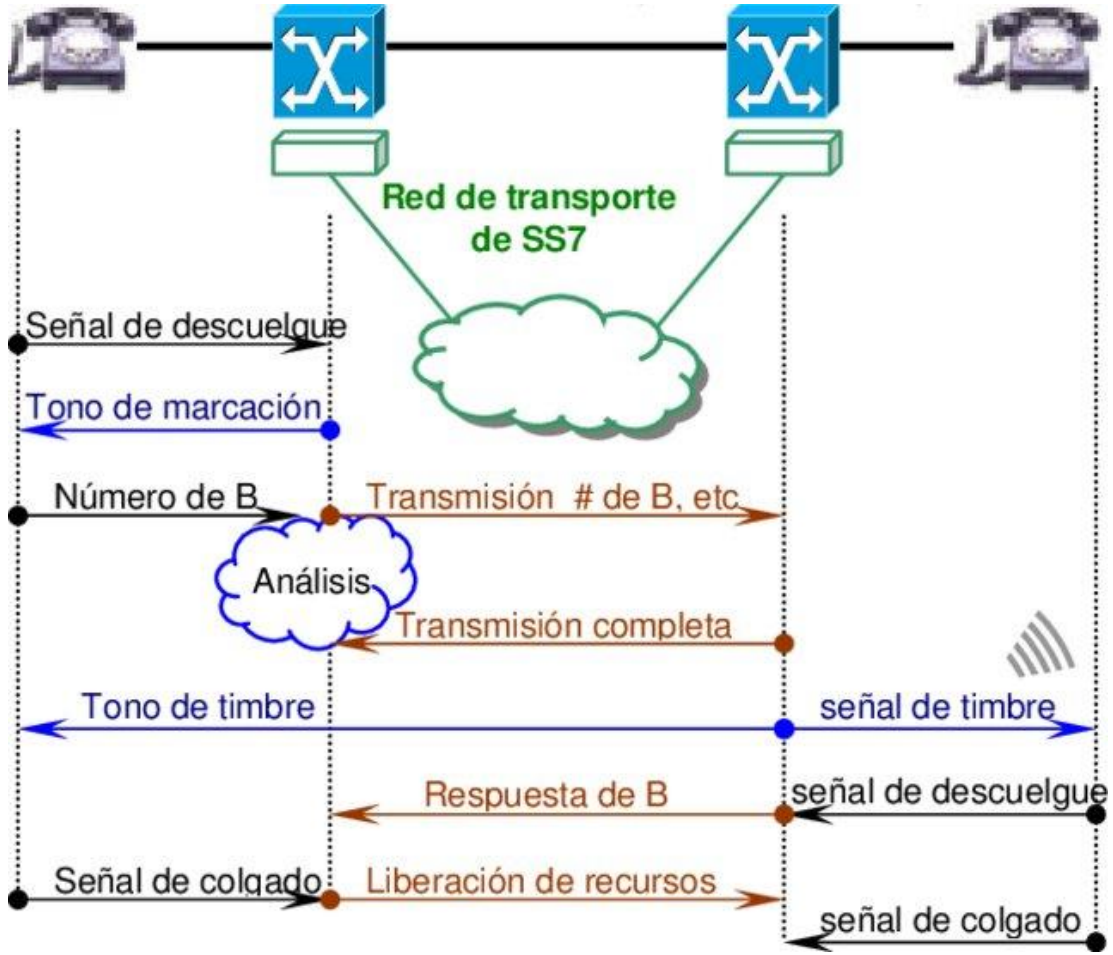
  - Ventaja
    - Se crea menos sobrecarga en la red.
  - Desventaja
    - Se da menor soporte al proceso de aplicación.

CONCEPTOS FUNDAMENTALES – Tipos de Servicios

- CON CONEXIÓN: Confiable / No confiable

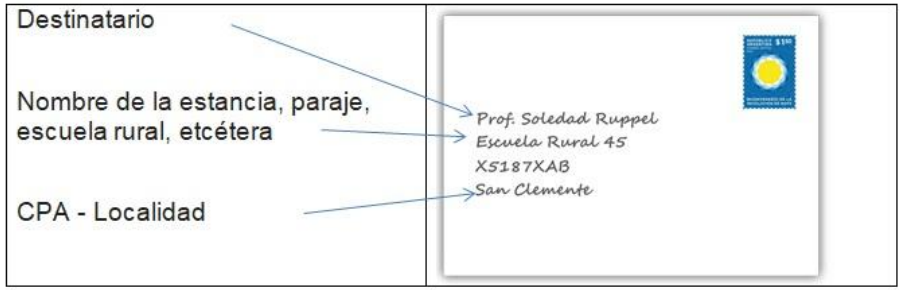
	Servicio	Ejemplo
Orientado a conexión	Flujo de mensajes confiable.	Secuencia de páginas.
	Flujo de bytes confiable.	Descarga de películas.
	Conexión no confiable.	Voz sobre IP.
Sin conexión	Datagrama no confiable.	Correo electrónico basura.
	Datagrama confirmación de recepción.	Mensajería de texto.
	Solicitud-respuesta.	Consulta en una base de datos.

Figura 1-16. Seis tipos distintos de servicios.



CONCEPTOS FUNDAMENTALES – Modelo de Capas

- SIN CONEXIÓN: Confiable / No confiable



	Servicio	Ejemplo
Orientado a conexión	Flujo de mensajes confiable.	Secuencia de páginas.
	Flujo de bytes confiable.	Descarga de películas.
	Conexión no confiable.	Voz sobre IP.
Sin conexión	Datagrama no confiable.	Correo electrónico basura.
	Datagrama confirmación de recepción.	Mensajería de texto.
	Solicitud-respuesta.	Consulta en una base de datos.

Figura 1-16. Seis tipos distintos de servicios.

MECANISMOS DE CONTROL DE TRÁFICO
CONEXIÓN - FLUJO – ERRORES - ACCESO AL MEDIO

- Protocolos de Gestión del Canal
  - Determinan qué estación puede usar el canal en cada momento.
  - **Protocolos Primario/Secundario** (Maestro/Esclavo)
    - Una estación gestiona el uso del canal
    - Ej. Sondeo/Selección
  - **Protocolos de Igual a Igual**
    - No hay una estación que controle el canal
    - Con prioridad o sin prioridad
    - Ej. 1. Paso de testigo – 2. Detección de portadora

MECANISMOS DE CONTROL DE TRÁFICO
CONEXIÓN - FLUJO – ERRORES - ACCESO AL MEDIO

- Protocolos Primario/Secundario
  - Sondeo/Selección:
    - Se adapta bien a redes con topología jerárquica
    - El equipo primario emplea dos tipos de órdenes:
      - Sondeo: pregunta al equipo secundario si tiene datos para enviar
      - Selección: avisa al equipo secundario de que le va a enviar datos
    - Todo el tráfico pasa por el equipo primario.

MECANISMOS DE CONTROL DE TRÁFICO
CONEXIÓN - FLUJO – ERRORES - ACCESO AL MEDIO

- Protocolos Primario/Secundario
  - Sondeo/Selección:
    - Problemas:
      - Cuello de botella en el equipo primario
      - Problema de fiabilidad si falla el equipo primario
      - El número de respuestas negativas puede ser muy alto
        - Tablas dinámicas de sondeo/selección

MECANISMOS DE CONTROL DE TRÁFICO
CONEXIÓN - FLUJO – ERRORES - ACCESO AL MEDIO

- Protocolos Primario/Secundario: Sondeo/Selección

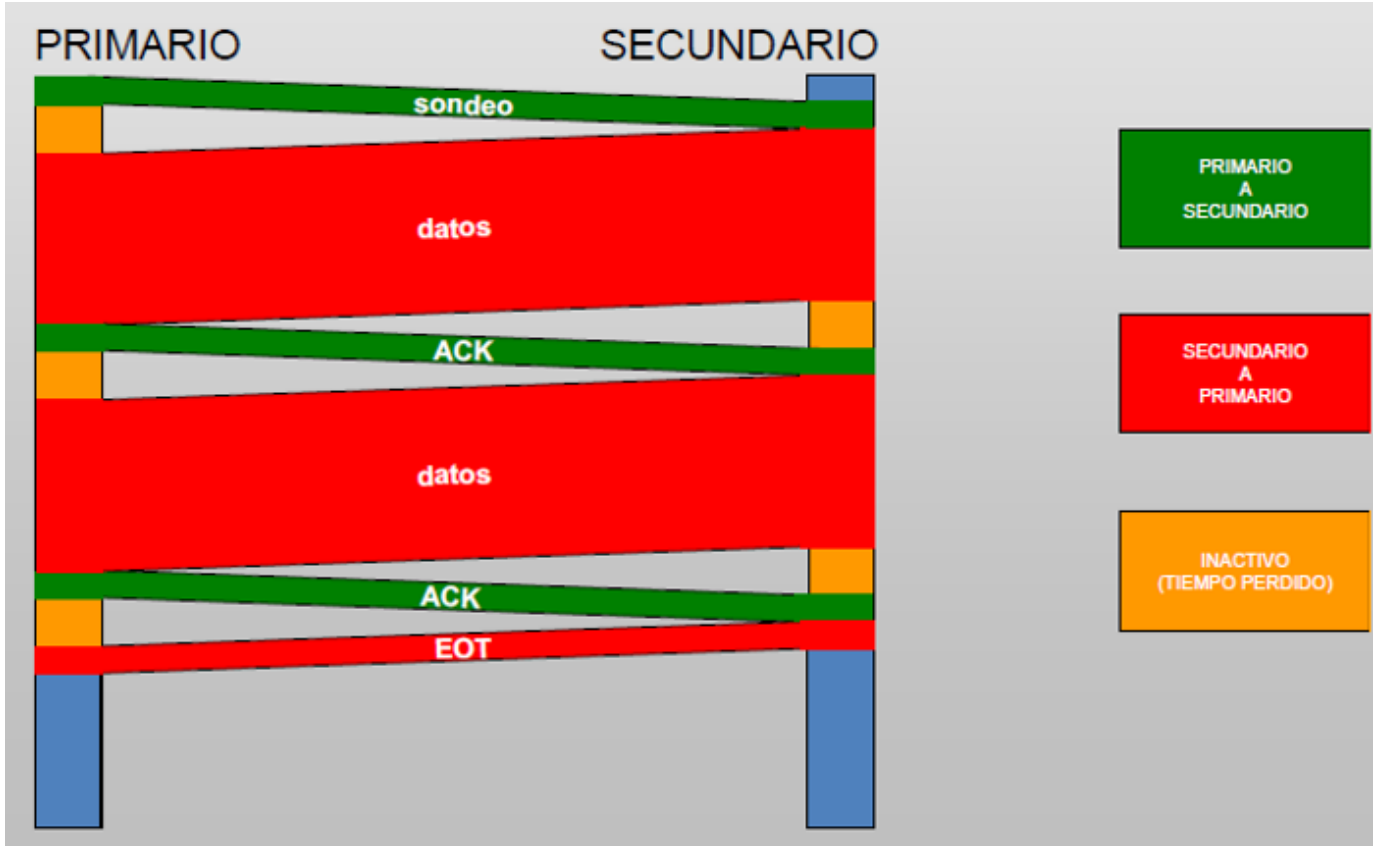
Problema	Solución
Error en la trama	Detección de errores Reconocimientos ACK y NAK
Pérdida de la trama Pérdida del reconocimiento	Espera cronometrada y retransmisión
Tramas duplicadas	Números de secuencia

MECANISMOS DE CONTROL DE TRÁFICO
CONEXIÓN - FLUJO – ERRORES - ACCESO AL MEDIO

- Protocolos Primario/Secundario
  - Sondeo/Selección con Parada y Espera:
    - La estación transmite una trama y espera respuesta
    - Válido para sistemas semidúplex
    - Económico
    - Problemas:
      - Bajo rendimiento.

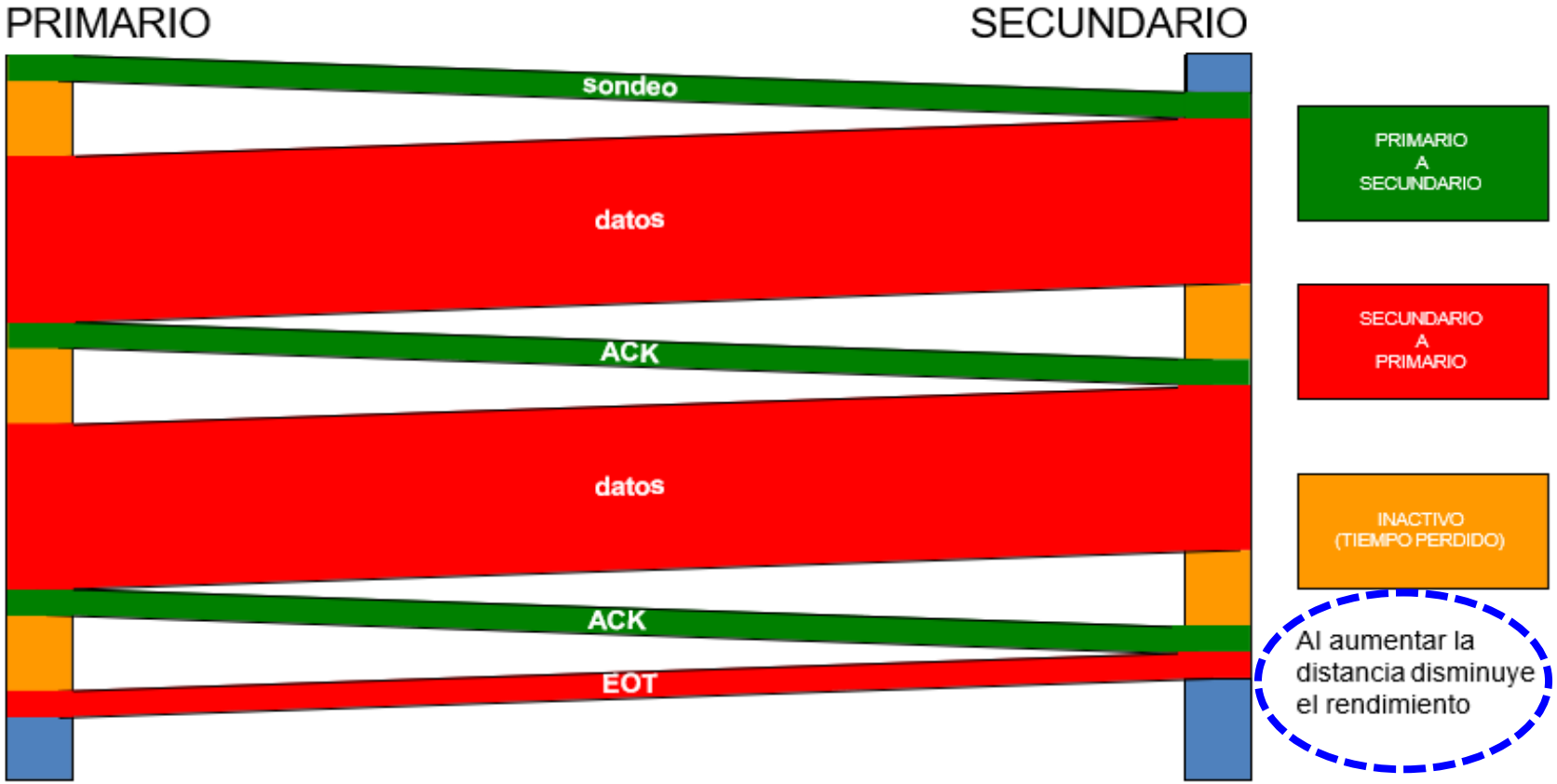
MECANISMOS DE CONTROL DE TRÁFICO
CONEXIÓN - FLUJO – ERRORES - ACCESO AL MEDIO

- **Protocolos Primario/Secundario: Sondeo/Selección con Parada y Espera**



MECANISMOS DE CONTROL DE TRÁFICO
CONEXIÓN - FLUJO – ERRORES - ACCESO AL MEDIO

- **Protocolos Primario/Secundario: Sondeo/Selección con Parada y Espera**



MECANISMOS DE CONTROL DE TRÁFICO
CONEXIÓN - FLUJO – ERRORES - ACCESO AL MEDIO

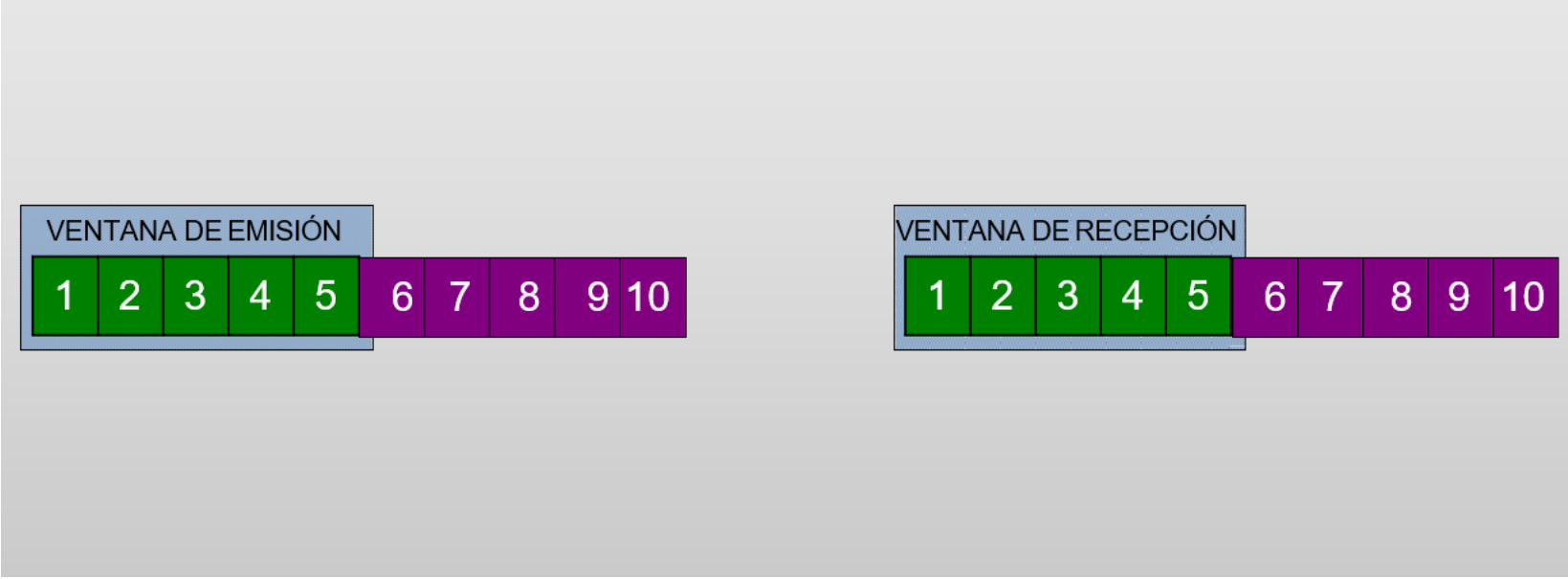
- **Protocolos Primario/Secundario: Sondeo/Selección con ARQ (Automatic Repeat-reQuest) continuo.**
  - **También llamado “Ventanas Deslizantes o Móviles”.**
    - La idea es permitir el envío de una trama antes de la llegada del reconocimiento de la anterior
    - Se reducen los tiempos perdidos de Parada y Espera
    - Válido en sistemas dúplex integral.
    - Ventanas EMISOR / RECEPTOR

MECANISMOS DE CONTROL DE TRÁFICO
CONEXIÓN - FLUJO – ERRORES - ACCESO AL MEDIO

- **Protocolos Primario/Secundario: Sondeo/Selección con ARQ (Automatic Repeat-reQuest) continuo.**

MECANISMOS DE CONTROL DE TRÁFICO
CONEXIÓN - FLUJO – ERRORES - ACCESO AL MEDIO

- **Protocolos Primario/Secundario: Sondeo/Selección con ARQ (Automatic Repeat-reQuest) continuo.**

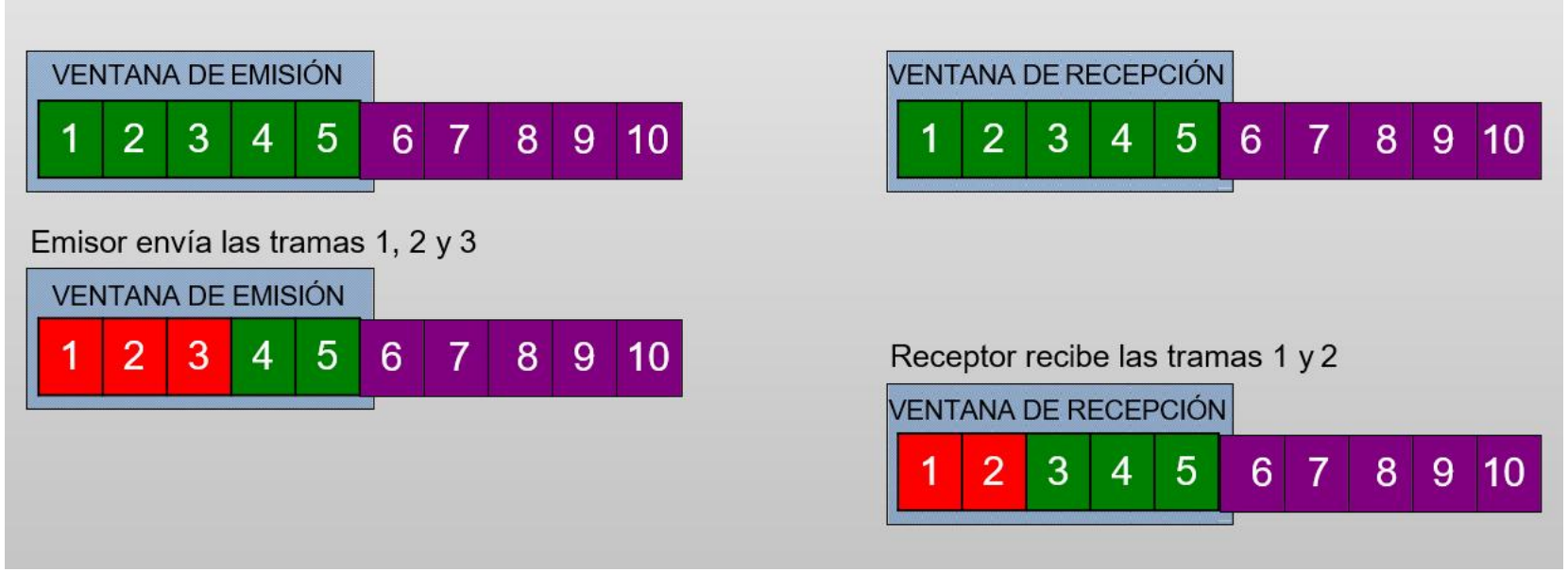


MECANISMOS DE CONTROL DE TRÁFICO
CONEXIÓN - FLUJO – ERRORES - ACCESO AL MEDIO

- **Protocolos Primario/Secundario: Sondeo/Selección con ARQ (Automatic Repeat-reQuest) continuo.**

MECANISMOS DE CONTROL DE TRÁFICO
CONEXIÓN - FLUJO – ERRORES - ACCESO AL MEDIO

- **Protocolos Primario/Secundario: Sondeo/Selección con ARQ (Automatic Repeat-reQuest) continuo.**



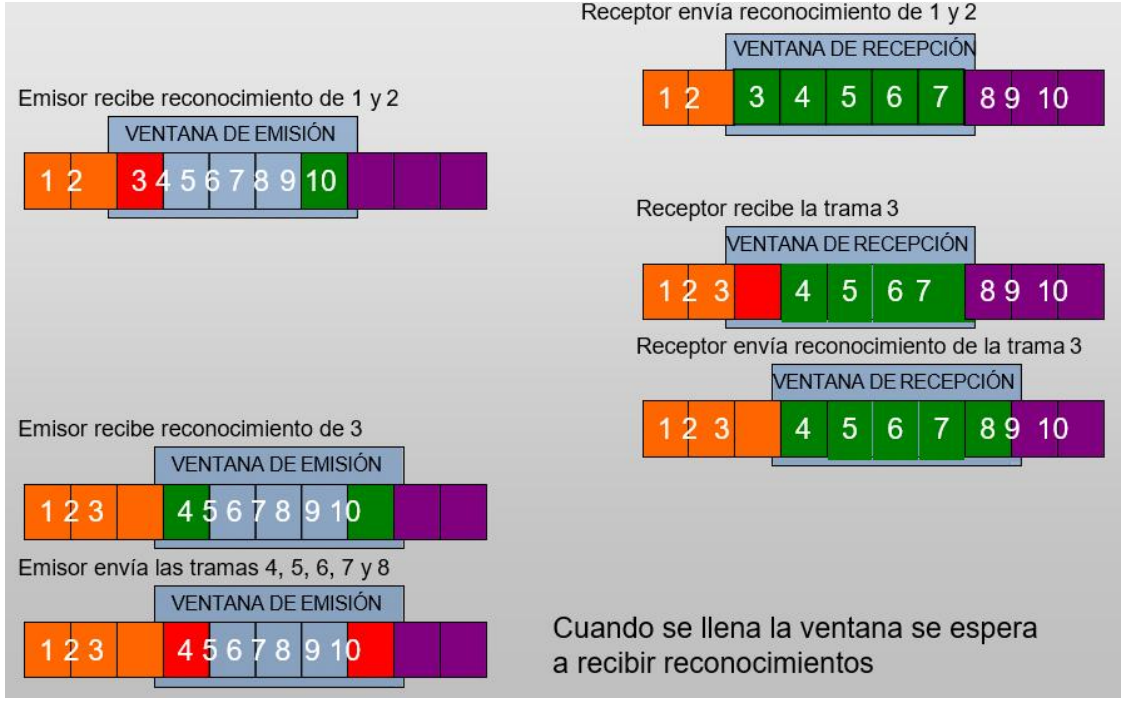
MECANISMOS DE CONTROL DE TRÁFICO
CONEXIÓN - FLUJO – ERRORES - ACCESO AL MEDIO

- **Protocolos Primario/Secundario: Sondeo/Selección con ARQ (Automatic Repeat-reQuest) continuo.**

MECANISMOS DE CONTROL DE TRÁFICO
CONEXIÓN - FLUJO – ERRORES - ACCESO AL MEDIO

- **Protocolos Primario/Secundario: Sondeo/Selección con ARQ (Automatic Repeat-reQuest) continuo.**

En algún momento, una de las ventanas se llena…



MECANISMOS DE CONTROL DE TRÁFICO
CONEXIÓN - FLUJO – ERRORES - ACCESO AL MEDIO

- **Protocolos Primario/Secundario: Sondeo/Selección con ARQ (Automatic Repeat-reQuest) continuo.**
  - **Se puede usar reconocimiento inclusivo para reducir el número de reconocimientos**
  - **En caso de error en alguna trama hay 2 maneras de actuar:**
    - **Rechazo o repetición no selectiva**
      - ❑ **Se descartan todas las tramas a partir de la errónea**
      - ❑ **No necesita almacenar tramas en espera ni reordenarlas**
      - ❑ **Exige la retransmisión de tramas que pudieron ser correctas**
    - **Repetición selectiva**
      - ❑ **Exige la retransmisión sólo de la trama errónea**
      - ❑ **El tamaño de la ventana de recepción ha de ser mayor que 1**
      - ❑ **Mayor consumo de recursos de almacenamiento**
      - ❑ **Es necesario reordenar las tramas**

MECANISMOS DE CONTROL DE TRÁFICO
CONEXIÓN - FLUJO – ERRORES - ACCESO AL MEDIO

- **Protocolos de Gestión del Canal**

  Determinan qué estación puede usar el canal en cada momento.

  - **Protocolos Primario/Secundario** (Maestro/Esclavo) ✓

    Una estación gestiona el uso del canal

    - Ej. Sondeo/Selección

  - **Protocolos de Igual a Igual**

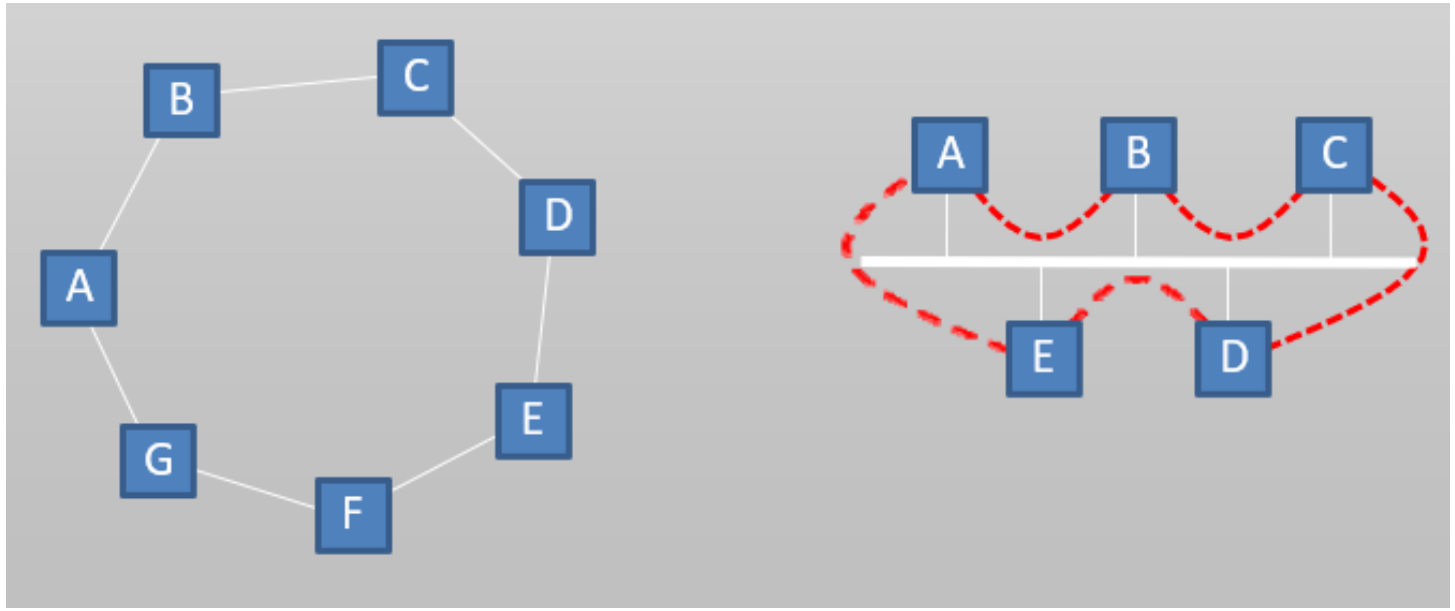
    No hay una estación que controle el canal

    Con prioridad o sin prioridad

    - Ej. 1. Paso de testigo - 2. Detección de portadora

MECANISMOS DE CONTROL DE TRÁFICO
CONEXIÓN - FLUJO – ERRORES - ACCESO AL MEDIO

- **Protocolos de Igual a Igual (CON / SIN PRIORIDAD): Paso de testigo en anillo**
  - **Empleado en redes con topología en anillo y en anillo lógico**
  - **El control de acceso al medio se realiza mediante una trama especial (testigo)**

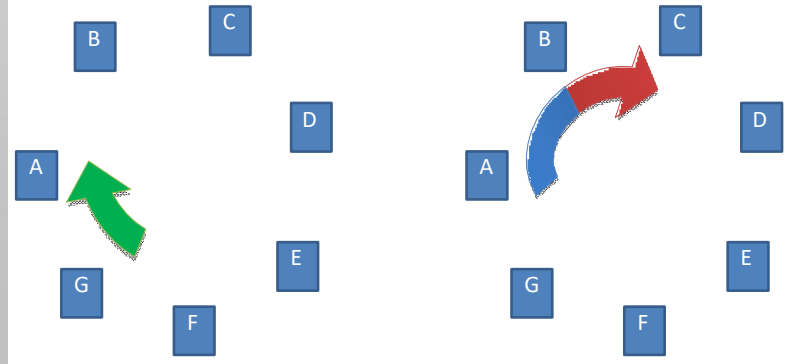


MECANISMOS DE CONTROL DE TRÁFICO
CONEXIÓN - FLUJO – ERRORES - ACCESO AL MEDIO

- **Protocolos de Igual a Igual (SIN PRIORIDAD): Paso de testigo en anillo**

- Flujo de datos en un único sentido
- El testigo puede estar en dos estados:
  - **Ocupado**: Alguna estación está transmitiendo
  - **Libre**: El canal está libre
    - Solo la estación que recibe el testigo libre puede transmitir. Para ello:
      - Marca el testigo como ocupado
      - Envía a la siguiente estación el testigo seguido de sus datos
      - Solo la estación destino lee los datos
      - La estación emisora al recibir de vuelta el testigo y los datos:
        - Elimina los datos
        - Marca el testigo como libre
        - Envía el testigo a la siguiente estación aunque quiera enviar más datos

- **Se evita que una estación monopolice el anillo**
- **En el anillo lógico se eliminan las colisiones**
- **Se pueden establecer prioridades**

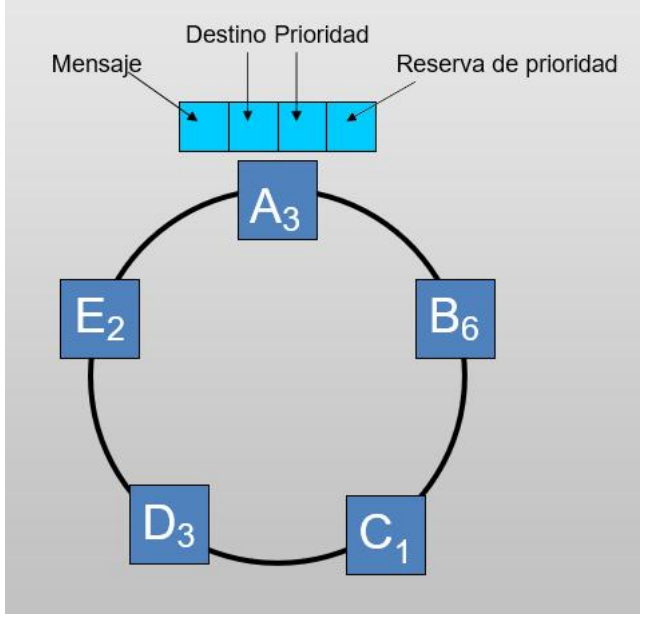


MECANISMOS DE CONTROL DE TRÁFICO
CONEXIÓN - FLUJO – ERRORES - ACCESO AL MEDIO

- **Protocolos de Igual a Igual (CON / SIN PRIORIDAD): Paso de testigo en bus**
  - **Empleado en topologías en bus**
  - **El acceso al medio se realiza como si se tratase de un anillo real**
  - **Se elimina la posibilidad de colisión**
  - **Cada estación sabe cuál es su sucesora**
  - **No es necesaria una ordenación específica de las estaciones**
  - **Solo quien posee el testigo puede usar el canal**
  - **Todas las estaciones escuchan el canal, pero solo la sucesora de la que emite "presta atención"**

MECANISMOS DE CONTROL DE TRÁFICO
CONEXIÓN - FLUJO – ERRORES - ACCESO AL MEDIO

- **Protocolos de Igual a Igual (CON / SIN PRIORIDAD): Paso de testigo con prioridad**
  - **Cada estación tiene asignada una prioridad de entre 8 posibles (ej. 1=máxima prioridad, 8=mínima prioridad)**
  - **El testigo tiene un campo *prioridad* y otro *reserva de prioridad***
    - **Una estación puede transmitir si tiene igual o mayor prioridad que la marcada en el testigo y el testigo está libre**
    - **Si el testigo está ocupado y se quiere reservar para la próxima transmisión**
      - ❑ **Sólo lo puede hacer si se tiene igual o mayor prioridad que la marcada en campo reserva de prioridad**
      - ❑ **Guarda la reserva de prioridad del testigo y pone su prioridad**
      - ❑ **Al terminar su transmisión pone en el testigo la reserva de prioridad que guardó**



MECANISMOS DE CONTROL DE TRÁFICO
CONEXIÓN - FLUJO – ERRORES - ACCESO AL MEDIO

- **Protocolos de Gestión del Canal**

  Determinan qué estación puede usar el canal en cada momento.

  - **Protocolos Primario/Secundario** (Maestro/Esclavo) ✓

    Una estación gestiona el uso del canal

    - Ej. Sondeo/Selección

  - **Protocolos de Igual a Igual**

    No hay una estación que controle el canal

    Con prioridad o sin prioridad

    - Ej. 1. Detección de portadora, 2. Paso de testigo

MECANISMOS DE CONTROL DE TRÁFICO
CONEXIÓN - FLUJO – ERRORES - ACCESO AL MEDIO

- **Protocolos de Igual a Igual (SIN PRIORIDAD): Escucha de Portadora con Detección de Colisión.**
  - **Antes de transmitir se escucha el canal:**
    - **Si está libre → transmitir**
    - **Si está ocupado → esperar**
  - **Si dos estaciones ven a la vez el canal libre, ambas empiezan a transmitir a la vez → colisión**
  - **Hay varios métodos para conseguir el control del canal teniendo en cuenta las colisiones:**
    - **Escucha de portadora 1-persistente**
    - **Escucha de portadora No-persistente**
    - **Escucha de portadora p-persistente**

MECANISMOS DE CONTROL DE TRÁFICO
CONEXIÓN - FLUJO – ERRORES - ACCESO AL MEDIO

Protocolos de Igual a Igual (SIN PRIORIDAD): Escucha de portadora 1-persistente

- **Antes de transmitir se escucha el canal:**
  - **Si está libre → transmitir**
  - **Si está ocupado → escucha continua y transmisión al quedar libre**
  - **Colisión → espera aleatoria y retransmisión**
- **Ventaja**
  - **Alta ocupación del canal**
- **Desventaja**
  - **Alto número de colisiones**

Protocolos de Igual a Igual (SIN PRIORIDAD): Escucha de portadora No-persistente

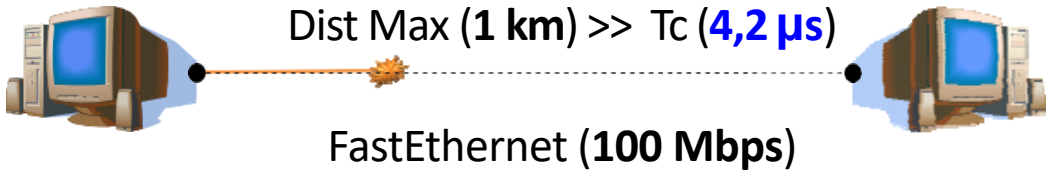
- **Antes de transmitir se escucha el canal:**
  - **Si está libre → transmitir**
  - **Si está ocupado → espera aleatoria y escucha**
  - **Colisión → espera aleatoria y retransmisión**
- **Ventaja**
  - **Bajo número de colisiones**
- **Desventaja**
  - **Baja ocupación del canal**

MECANISMOS DE CONTROL DE TRÁFICO
CONEXIÓN - FLUJO – ERRORES - ACCESO AL MEDIO

- **Protocolos de Igual a Igual (SIN PRIORIDAD): Escucha de Portadora p-persistente.**
  - **Se divide el tiempo en intervalos de una trama**
    - **Si está libre → transmitir en el intervalo actual con probabilidad P, esperar al siguiente intervalo con probabilidad 1-p**
    - **Si está ocupado → espera aleatoria y escucha**
    - **Colisión → espera aleatoria y retransmisión**
  - **Compromiso entre la alta ocupación del canal y el bajo número de colisiones**

MECANISMOS DE CONTROL DE TRÁFICO
CONEXIÓN - FLUJO – ERRORES - ACCESO AL MEDIO

- **Protocolos de Igual a Igual (SIN PRIORIDAD): Escucha de Portadora p-persistente.**
  - **Ventana de colisión (Vc)**
    - **Retardo de la propagación de la señal**
    - **Distancia entre las estaciones**
    - **Durante unos instantes una estación ve libre el canal, aunque esté ocupado → colisión**
    - **Al aumentar la ventana de colisión se incrementa el número de colisiones**
    - **El sistema de escucha de portadora no es adecuado en WAN por el gran tamaño de la ventana de colisión**
    - **Ejemplo:**



MECANISMOS DE CONTROL DE TRÁFICO

CONEXIÓN - FLUJO – ERRORES - ACCESO AL MEDIO -

1. Encapsulamiento.
2. Fragmentación y reensamblado.
3. **Control de conexión.**
4. Entrega ordenada.
5. **Control de flujo.**
6. **Control de errores.**
7. Direccionamiento.
8. Multiplexación.
9. **Servicios de transmisión**

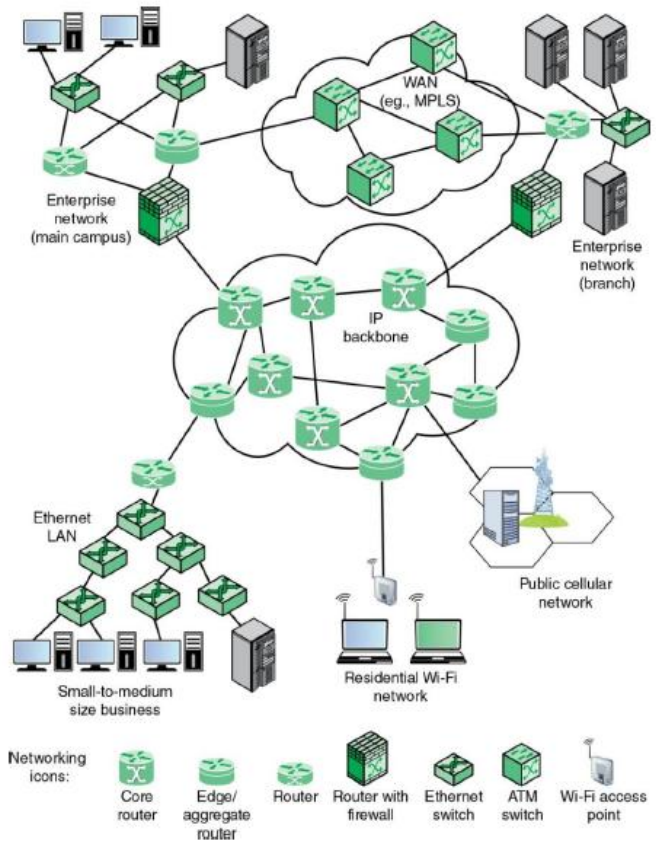


FIGURE 1.2 A Global Networking Architecture

MECANISMOS DE CONTROL DE TRÁFICO
FLUJO - ACCESO

1. Encapsulamiento.
2. Fragmentación y reensamblado.
3. Control de conexión.
4. Entrega ordenada.
5. **Control de flujo.**
6. Control de errores.
7. Direccionamiento.
8. Multiplexación.
9. Servicios de transmisión.

- **Sistemas sin sondeo:**
  - Flujo de software XON/XOFF: los controles de flujo de transmisor encendido/transmisor apagado (XON/XOFF) implican el envío de caracteres de control de transmisión de datos a lo largo de la corriente de datos (TxD y RxD).
  - Flujo de hardware RTS/CTS: la solicitud de enviar/borrar para enviar (RTS/CTS) se denomina a veces ritmo o reconocimiento de hardware en lugar de control de flujo. También se utiliza en redes WIFI; el estándar 802.11 incluye la función de umbral RTS (Request to Clear) con CTS (Clear to Send) para controlar el acceso de la estación al medio inalámbrico.
  - Flujo de hardware DTR/DSR: el terminal de datos preparado (DTR), otra forma de control de flujo de hardware, lo generan normalmente los dispositivos, como las impresoras, para indicar que están preparados para comunicarse con el sistema. Esta señal se utiliza junto con Conjunto de datos preparado (DSR) que el sistema genera para controlar el flujo de datos.

MECANISMOS DE CONTROL DE TRÁFICO

Diferencia entre RTS/CTS y DTR/DSR

Solicitud de envío / Autorización para enviar:
RTS/CTS es un mecanismo de flujo en el que el equipo terminal de datos (DTE) aloja activos o envía RTS al equipo de comunicación de datos (DCE). **Se usa para indicar que el host está listo para enviar datos y el módem puede iniciar o formar un canal de comunicación. Luego, DCE confirma o envía CTS para otorgar permiso y puede enviar datos.**
RTS simplemente indica que el host desea enviar algunos datos, mientras que CTS simplemente indica que sí puede comenzar a enviar datos. Aquí, el host puede ser una computadora o cualquier otro dispositivo y el DCE puede ser un módem.

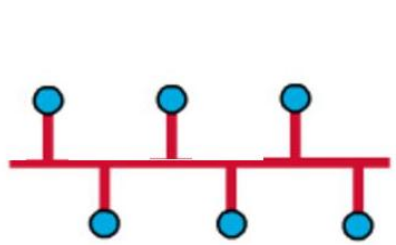
RTS/CTS	DTR/DSR
Al usar RTS/CTS, hay mucho almacenamiento en búfer por hardware.	Mientras se usa el control de flujo DTR/DSR, no hay almacenamiento en búfer.
Se utiliza en diferentes campos como el Académico, Vending, Industrial, etc.	Se utiliza en diferentes campos como POS (Punto de Venta), Impresoras, EPOS (Punto de Venta Electrónico), etc.
También se puede utilizar para controlar el flujo de datos entre el host y el dispositivo.	También se puede usar para controlar el flujo de datos, el protocolo de enlace y también para proporcionar energía.
RTS simplemente indica que quiere enviar datos al dispositivo que se está conectando.	DTR simplemente indica que el dispositivo que se está conectando está listo para recibir datos.
RTS solo inicia y detiene la comunicación.	DTR también indica que hay algunos equipos presentes.
Las líneas RTS/CTS no están controladas por firmware. En cambio, están controlados y dirigidos por hardware.	Las líneas DTR/DSR generalmente se controlan mediante firmware en adaptadores.

Terminal de datos listo / Conjunto de datos listo:

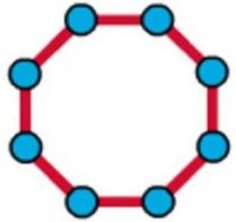
DTR/DSR es un mecanismo de flujo en el que el DTE, es decir, el host, afirma o envía DTR al DCE, es decir, el módem, simplemente **para indicar que el host está listo para recibir la comunicación y el módem puede iniciar o crear un canal de comunicación.**

Luego, el DCE activa además DSR para indicar simplemente que el receptor está listo para la comunicación.

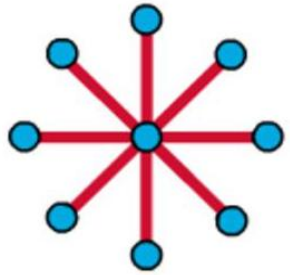
TOPOLOGÍAS LAN Y WAN



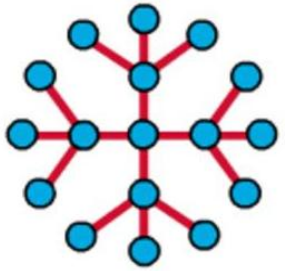
Topología de bus



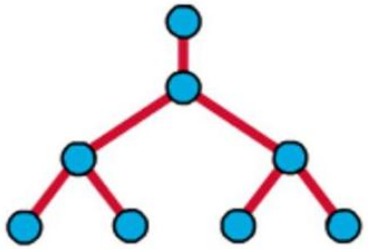
Topología de anillo



Topología en estrella



Topología en estrella extendida



Topología jerárquica

Topología en malla

LAN

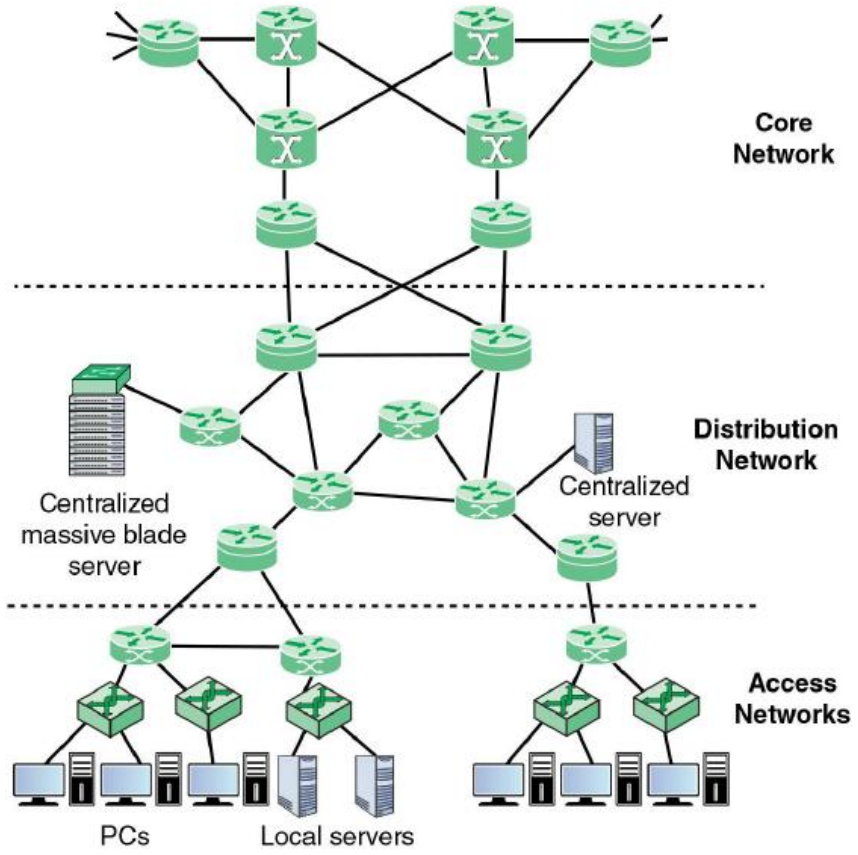
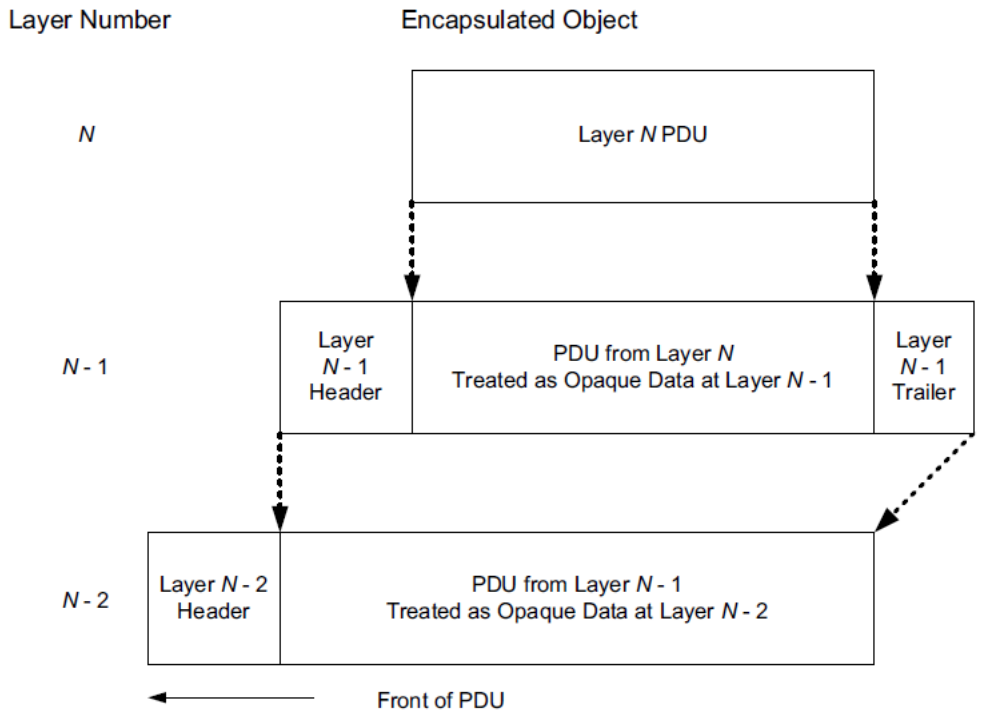


FIGURE 1.3 A Typical Network Hierarchy

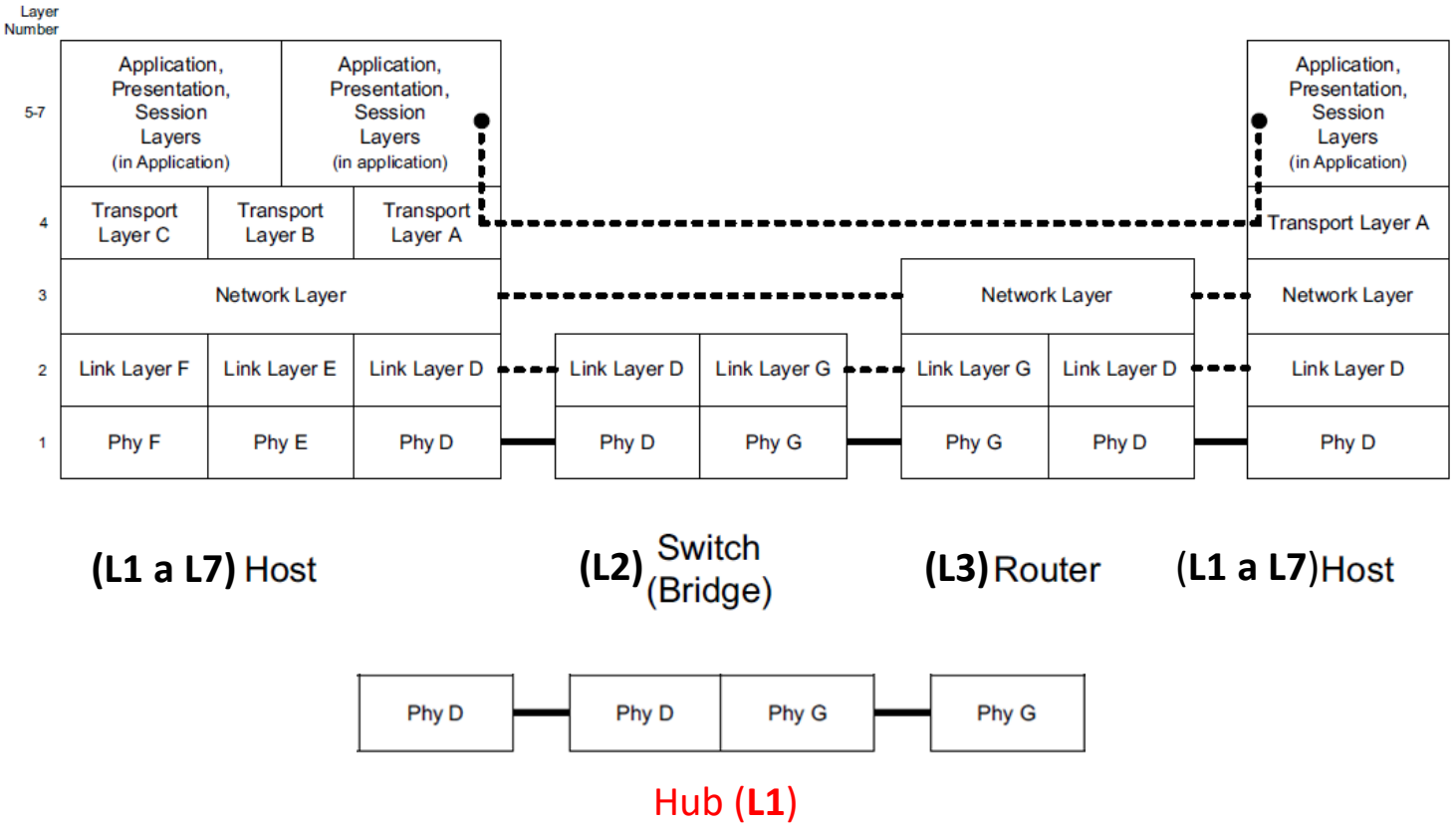
- Topología y Diseño Físico.
- VLANs y Diseño Lógico.
- Estándares IEEE 802.2, 802.3, 802.1Q, 802.11, EIA/TIA 568
- Organización:
  - Jerarquía funcional en LAN: Acceso – Distribución - Núcleo.
  - Políticas y servicios.
  - Microsegmentación y Seguridad Cibernética.

ENCAPSULAMIENTO (PCI/ICI – SDU – PDU)



- El encapsulamiento se utiliza generalmente junto con el modelo de capas (Cliente / Servidor)
- El encapsulamiento puro implica tomar la PDU de una capa y tratarla como datos opacos (no interpretados) en la capa abajo.
- El encapsulamiento se lleva a cabo en cada remitente y su desencapsulamiento (la operación inversa) tiene lugar en cada receptor.
- La mayoría de los protocolos utilizan encabezados durante el encapsulamiento; algunos, también, utilizan “colas”.

ARQUITECTURA Y CONMUTACIÓN (BRIDGING / ROUTING)



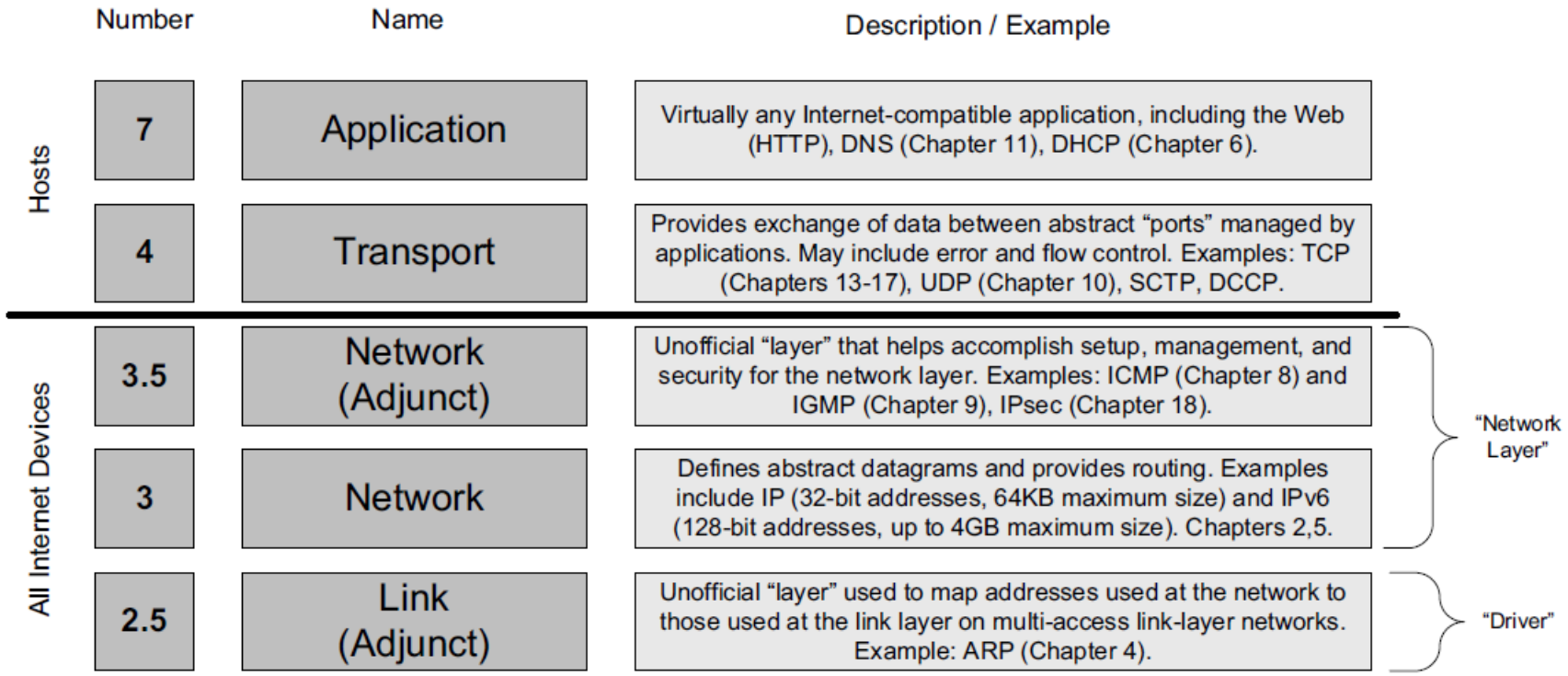
- Diferentes dispositivos de red implementan diferentes subconjuntos de la pila de protocolos.
- Los anfitriones finales tienden a implementar todas las capas.
- Los enrutadores implementan capas debajo de la capa de transporte y los conmutadores implementan protocolos de capa de enlace y siguientes.
- Esta estructura idealizada a menudo se viola porque los enrutadores y los conmutadores generalmente incluyen la capacidad de actuar como un host (por ejemplo, para ser administrados y configurados) y, por lo tanto, necesitan una implementación de todas las capas incluso si rara vez se utilizan.

MODELO DE REFERENCIA OSI

	Number	Name	Description/Example
Hosts	7	Application	Specifies methods for accomplishing some user-initiated task. Application-layer protocols tend to be devised and implemented by application developers. Examples include FTP, Skype, etc.
	6	Presentation	Specifies methods for expressing data formats and translation rules for applications. A standard example would be conversion of EBCDIC to ASCII coding for characters (but of little concern today). Encryption is sometimes associated with this layer but can also be found at other layers.
	5	Session	Specifies methods for multiple connections constituting a communication session. These may include closing connections, restarting connections, and checkpointing progress. ISO X.225 is a session-layer protocol.
	4	Transport	Specifies methods for connections or associations between multiple programs running on the same computer system. This layer may also implement reliable delivery if not implemented elsewhere (e.g., Internet TCP, ISO TP4).
All Networked Devices	3	Network or Internetwork	Specifies methods for communicating in a multihop fashion across potentially different types of link networks. For packet networks, describes an abstract packet format and its standard addressing structure (e.g., IP datagram, X.25 PLP, ISO CLNP).
	2	Link	Specifies methods for communication across a single link, including "media access" control protocols when multiple systems share the same media. Error detection is commonly included at this layer, along with link-layer address formats (e.g., Ethernet, Wi-Fi, ISO 13239/HDLC).
	1	Physical	Specifies connectors, data rates, and how bits are encoded on some media. Also describes low-level error detection and correction, plus frequency assignments. We mostly stay clear of this layer in this text. Examples include V.92, Ethernet 1000BASE-T, SONET/SDH.

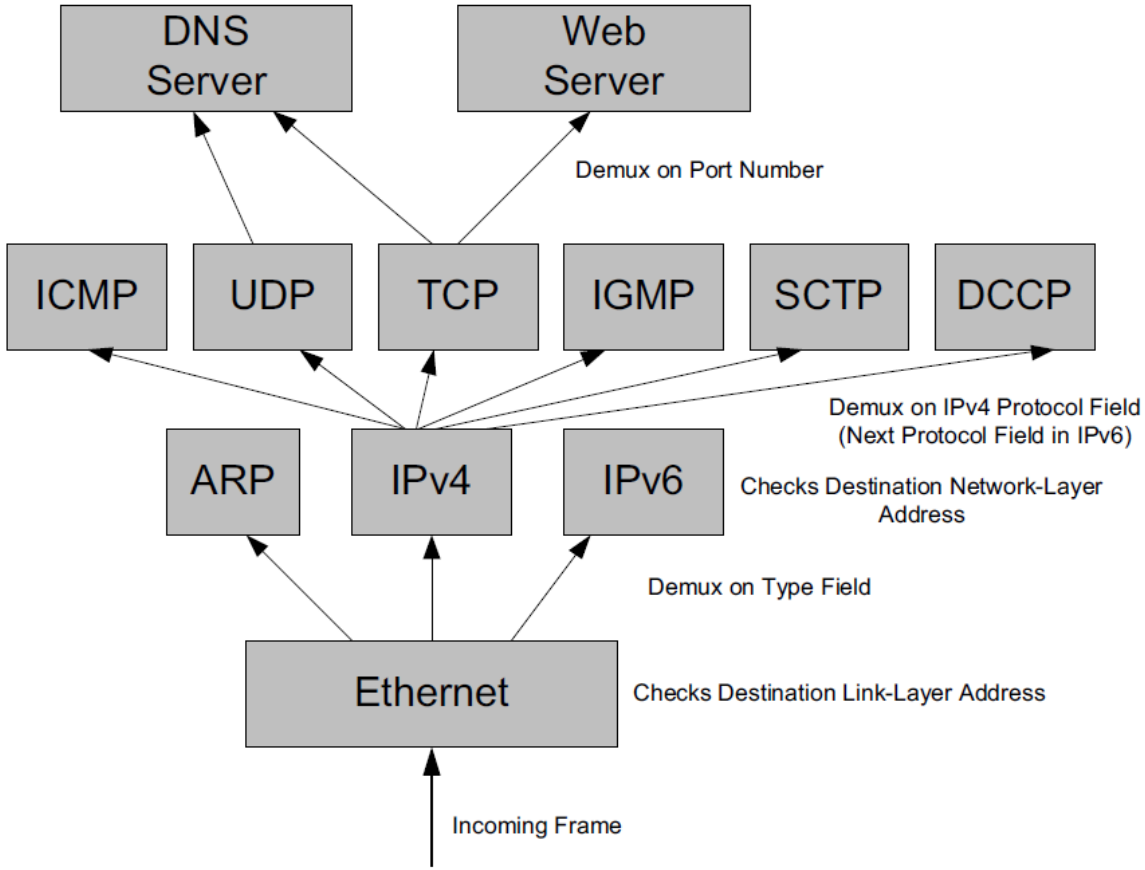
Figure 1-2 The standard seven-layer OSI model as specified by the ISO. Not all protocols are implemented by every networked device (at least in theory). The OSI terminology and layer numbers are widely used.

MODELO DE REFERENCIA ARPANET - SUITE TCP/IP



- Capas de protocolo basadas en la suite TCP/IP utilizada en Internet.
- No hay capas Sesión y Presentación.
- Además, existen varios protocolos "adjuntos" o auxiliares que no encajan exactamente en las capas estándares, pero realizan funciones críticas para el funcionamiento de los otros protocolos.
- Algunos de estos protocolos no se utilizan con IPv6 (por ejemplo, IGMP y ARP).

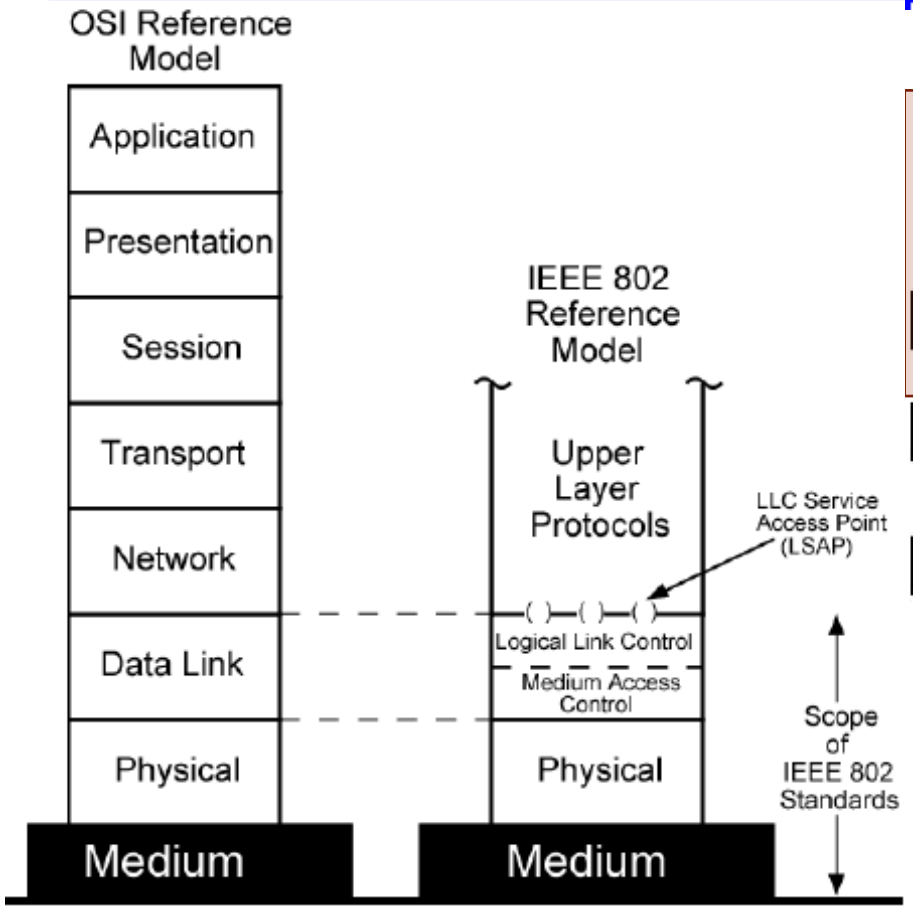
MULTIPLEXACIÓN, DEMULTIPLEXACIÓN, ENCAPSULAMIENTO Y CONTROL DE ERRORES EN TCP/IP



- Utiliza una combinación de información de direccionamiento y demultiplexación de protocolos.
- Emplea identificadores para determinar si un datagrama se ha recibido correctamente y, de ser así, qué entidad debe procesarlo.
- Varias capas también verifican valores numéricos (por ejemplo, sumas de verificación) para garantizar que el contenido no haya sufrido daños durante el transporte.

MODELOS Y ARQUITECTURAS: FUNCIONES Y MECANISMOS

IEEE 802 v OSI



Protocolos TCP/IP