

01130  
9



# UNIVERSIDAD NACIONAL AUTÓNOMA DE MÉXICO

FACULTAD DE INGENIERIA  
DIVISIÓN DE INGENIERIA ELECTRICA

DISEÑO E IMPLEMENTACIÓN DEL LABORATORIO DE DATOS  
DE LA FACULTAD DE INGENIERIA.

**T E S I S**

PARA OBTENER EL TITULO DE:

**INGENIERO EN TELECOMUNICACIONES**

P R E S E N T A N :

**RAFAEL CANSIGNO PELÁEZ**

**VÍCTOR MANUEL ROSALES CONSUELOS**



MEXICO, D. F., CIUDAD UNIVERSITARIA,

2003

A handwritten mark resembling a stylized letter 'A' or a similar symbol.



Universidad Nacional  
Autónoma de México



**UNAM – Dirección General de Bibliotecas**  
**Tesis Digitales**  
**Restricciones de uso**

**DERECHOS RESERVADOS ©**  
**PROHIBIDA SU REPRODUCCIÓN TOTAL O PARCIAL**

Todo el material contenido en esta tesis esta protegido por la Ley Federal del Derecho de Autor (LFDA) de los Estados Unidos Mexicanos (México).

El uso de imágenes, fragmentos de videos, y demás material que sea objeto de protección de los derechos de autor, será exclusivamente para fines educativos e informativos y deberá citar la fuente donde la obtuvo mencionando el autor o autores. Cualquier uso distinto como el lucro, reproducción, edición o modificación, será perseguido y sancionado por el respectivo titular de los Derechos de Autor.

**Temario de la tesis.**

**Diseño e implementación del laboratorio de datos de la Facultad de Ingeniería.**

**Primera parte.**

**Capítulo 1. Aspectos teóricos fundamentales para el entendimiento, uso y aplicación de las redes de datos.**

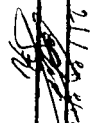
- 1.1 Principios y necesidades del uso de redes de datos.
- 1.2 Definición.
- 1.3 Ventajas de usar redes de datos.
- 1.4 Una de las aplicaciones más exitosas de las redes de datos (Internet).
- 1.5 Estandarización.
- 1.6 Modelo de referencia OSI.
  - 1.6.1 Capa física.
  - 1.6.2 Capa de enlace.
  - 1.6.3 Capa de red.
  - 1.6.4 Capa de transporte.
  - 1.6.5 Capa de sesión.
  - 1.6.6 Capa de presentación.
  - 1.6.7 Capa de aplicación.
- 1.7 Estructura de un sistema de Comunicaciones de datos.
- 1.8 Topologías de red.
- 1.9 Resumen.

**Capítulo 2. Medios de transmisión.**

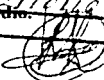
- 2.1 Introducción
- 2.2 Cable coaxial.
  - 2.2.1 Ethernet (Uso del cable coaxial en redes de datos)
  - 2.2.2 Cable Modem
  - 2.2.3 G.703.
  - 2.2.4 G.753.
- 2.3 Par trenzado.
  - 2.3.1 Ethernet (Uso del par trenzado en redes de datos)
  - 2.3.2 xDSL y DS0's
- 2.4 Fibra óptica.
  - 2.4.1 Ethernet (Uso de la fibra óptica en redes de datos)
  - 2.4.2 FDDI
  - 2.4.3 SDH
  - 2.4.4 ATM
- 2.5 Espacio Libre
- 2.6 Resumen.

**Capítulo 3. Tecnologías LAN.**

- 3.1 Introducción.
- 3.2 Logical Link Control (LLC), IEEE 802.2
- 3.3 MAC (Medium Access Control) o Control de Acceso al Medio.
- 3.4 Ethernet, Fast Ethernet, Gigabit Ethernet.
- 3.4.1 Ethernet.

Autorizo a la Dirección General de Bibliotecas de la UNAM a difundir en formato electrónico e impreso el contenido de mi trabajo recepcional.  
NOMBRE: Rafael Castañeda  
Fecha: 21/05/2003  
FIRMA: 

Autorizo a la Dirección General de Bibliotecas de la UNAM a difundir en formato electrónico e impreso el contenido de mi trabajo recepcional.

NOMBRE: Rafael Castañeda  
Fecha: 21/05/03  
FIRMA: 

- 3.4.1.1 Topología.
- 3.4.1.2 Implementación física.
- 3.4.1.3 Técnica de acceso al medio (CSMA/CD).
- 3.4.1.4 Formato de frame.
  - 3.4.1.4.1 Frame ethernet versión 2.
  - 3.4.1.4.2 IEEE 802.3.
  - 3.4.1.4.3 Novell (raw).
  - 3.4.1.4.4 SNAP.
- 3.4.2 Fast Ethernet.
  - 3.4.2.1 Implementación Física.
  - 3.4.2.2 Autonegociación.
- 3.4.3 Gigabit Ethernet.
- 3.4.3.1 Implementación Física.
- 3.5 FDDI.
- 3.5.1 FDDI o interfaz de datos distribuidos por fibra (Fiber Distributed Data Interface).
- 3.5.2 Topología.
- 3.5.3 Tolerancia a fallas.
  - 3.5.3.1 WRAP.
  - 3.5.3.2 Bypass.
  - 3.5.3.3 Dual Homing.
- 3.5.4 Arquitectura.
  - 3.5.4.1 PMD o Physical Media Dependent (dependencia del medio fisico).
    - 3.5.4.1.2 Funciones del PMD.
    - 3.5.4.1.3 Conector Medio-Interface.
      - 3.5.4.1.4 Tipos de puertos.
      - 3.5.4.1.5 Derivador óptico (Relay Bypass Optico).
    - 3.5.4.2 PHY o Physical Layer Protocol (protocolo de la capa fisica).
      - 3.5.4.2.1 Proceso de Codificación.
      - 3.5.4.2.2 Símbolos.
        - 3.5.4.2.2.1 Símbolo de estado de línea.
        - 3.5.4.2.2.2 Símbolos Indicadores de Control.
      - 3.5.4.2.3 MAC o Media Access Control (control de acceso al medio).
        - 3.5.4.2.3.1 Control de Acceso al Medio.
        - 3.5.4.2.3.2 Clases de servicio: síncrono y asíncrono.
        - 3.5.4.2.3.3 Definición de Tramas MAC.
      - 3.5.4.2.4 SMT o Station Management (gestión de estaciones).
- 3.5 Resúmen.

## Capítulo 4. Tecnologías WAN.

- 4.1 Definición.
- 4.2 Redes de conmutación de circuitos y conmutación de paquetes.
  - 4.2.1 Redes de Conmutación de Circuitos.
  - 4.2.2 Redes de Conmutación de Paquetes.
- 4.3 Capa Física: WAN.
  - 4.3.1 Tipos de interfaces.
  - 4.4 Tipos de conexiones WAN.
    - 4.4.1 Enlaces dedicados (Conexiones dedicadas).
    - 4.4.2 Enlaces vía circuitos virtuales.
    - 4.4.3 Enlaces conmutados.
- 4.5 Protocolos WAN usados sobre conexiones WAN dedicadas y conmutadas.
  - 4.5.1 SDLC y derivados.
    - 4.5.1.1 Topologías.



- 4.5.1.2 Formato de la trama de SDLC.
- 4.5.1.3 SDLC bit-stuffing.
- 4.5.1.4 Modos de operación.
- 4.5.2 HDLC.
- 4.5.3 LAPP.
- 4.5.4 PPP.
  - 4.5.4.1 Configuración básica.
  - 4.5.4.2 Entramado.
  - 4.5.4.3 Operación del PPP.
  - 4.5.4.4 Fases de la operación.
  - 4.5.4.5 Fase de enlace muerto (cupa física no lista).
  - 4.5.4.6 Fase de establecimiento del enlace.
  - 4.5.4.7 Fase de validación.
  - 4.5.4.8 Fase de red.
  - 4.5.4.9 Fase abierta.
  - 4.5.4.10 Fase de terminación del enlace.
  - 4.5.4.11 Negociación automática de opciones.
- 4.5.5 Anchos de banda en WAN's.
- 4.5.6 Tecnologías para el establecimiento de conexiones usando enlaces conmutados.
  - 4.5.6.1 Red telefónica.
  - 4.5.6.2 ISDN (Red Digital de Servicios Integrados).
    - 4.5.6.2.1 Definición de la Red Digital de Servicios Integrados (ISDN).
    - 4.5.6.2.2 Generalidades de ISDN.
    - 4.5.6.2.3 Centrales ISDN.
    - 4.5.6.2.4 Línea de transmisión.
    - 4.5.6.2.5 ISDN de banda estrecha.
    - 4.5.6.2.6 Acceso Básico (2B+D).
    - 4.5.6.2.7 Acceso Primario. (30B+D).
    - 4.5.6.2.8 Configuración de referencia.
    - 4.5.6.2.9 Agrupaciones funcionales.
    - 4.5.6.2.10 Puntos de referencia o interfaces.
    - 4.5.6.2.11 Numeración ISDN.
    - 4.5.6.2.12 Servicios de la ISDN.
    - 4.5.6.2.13 Teleservicios.
    - 4.5.6.2.14 Servicios suplementarios.
- 4.6.1 Frame Relay.
  - 4.6.1.1 Definición.
    - 4.6.1.2 Estandarización de Frame Relay.
  - 4.6.1.3 Dispositivos conectados en una red Frame Relay.
  - 4.6.1.4 Circuitos Virtuales Frame Relay.
  - 4.6.1.5 Circuitos Virtuales Conmutados (SVC o switched virtual circuit).
  - 4.6.1.6 Circuitos Virtuales Permanentes (PVC o private virtual circuit).
  - 4.6.1.7 Identificador de Conexión del Enlace de Datos (DLCI)(Data Link Conection Identifier).
  - 4.6.1.8 Mecanismos de control de saturación.
  - 4.6.1.9 BIT DE (Descart Elegibility).
  - 4.6.1.10 Verificación de errores en frame relay.
    - 4.6.1.11 Interfase LMI.
    - 4.6.1.12 Formato de la trama de Frame Relay.
    - 4.6.1.13 Formato de la trama LMI.
- 4.6.2 ATM.
  - 4.6.2.1 Definición.
  - 4.6.2.2 Modelo de Referencia ATM.

- 
- 4.6.2.2.1 Nivel Físico.
  - 4.6.2.2.2 Nivel ATM.
  - 4.6.2.2.3 Nivel de Adaptación ATM (AAL).
  - 4.6.2.2.4 Clases de Servicios.
  - 4.6.2.2.5 Servicios sin conexión ATM.
  - 4.6.2.2.6 Comunicaciones de datos sobre ATM - AAL5 (SEAL).
  - 4.6.2.3 Ventajas y desventajas que ofrecen estas tecnologías de conexión por medio de circuitos virtuales.
  - 4.6.2.3.1 Velocidad de acceso.
  - 4.6.2.3.2 Consideración de la calidad de servicio.
  - 4.6.2.3.3 Costos y acceso.
  - 4.6.2.3.4 Interconexión de redes LAN.
  - 4.6.3 Conclusiones de los diferentes enlaces existentes.
  - 4.7 Resumen

## Capítulo 5. Red.

- 5.1 Introducción.
- 5.2.1 Direccionamiento IP.
  - 5.2.1.1 Dirección IP.
  - 5.2.1.2 Clases de direcciones IP.
  - 5.2.1.3 Direcciones IP especiales y reservadas.
  - 5.2.1.4 Máscara de subred.
  - 5.2.1.5 Generación de subredes.
  - 5.2.1.6 Máscara de Subred de Longitud Variable (VLSM).
  - 5.2.1.7 Direccionamiento sin clase CIDR (Classless Inter - Domain Routing).
  - 5.2.1.8 Protocolo IP.
  - 5.2.1.9 Formato del datagrama IP.
  - 5.2.1.10 Fragmentación MTU (Maximum Transfer Unit).
- 5.3.1.1 Routing information Protocol (RIP).
  - 5.3.1.1.1 Estructura del Frame de RIP.
  - 5.3.1.2 Protocolo RIP v2.
- 5.3.2 Interior Gateway Routing Protocol (IGRP).
- 5.3.3 Protocolo OSPF (Open Shortest Path First).
  - 5.3.3.1 El protocolo OSPF.
  - 5.3.3.2 Áreas y Dominio de enrutamiento OSPF.
  - 5.3.3.3 Backbone OSPF.
  - 5.3.3.4 Clasificación de los enrutadores OSPF.
  - 5.3.3.5 Vecinos y Adyacencias.
  - 5.3.3.6 Enrutador Designado y Enrutador Designado de Respaldo.
  - 5.3.3.7 Estructura de un paquete OSPF.
- 5.4 Resumen.

## Segunda Parte.

### Capítulo 6. Aspectos lógicos y físicos del Laboratorio de Redes. Diseño del laboratorio en condiciones ideales y ejemplos de implementación.

- 6.1 Introducción.
- 6.2 Racks.
- 6.3 Mueblería adicional para ubicación de equipo didáctico.
- 6.4 Piso del laboratorio

- 
- 6.5 Muros y techo.
  - 6.6 Iluminación
  - 6.7 Clima.
  - 6.8 Humedad relativa.
  - 6.9 Temperatura en el laboratorio.
  - 6.10 Aire acondicionado.
  - 6.11 Requerimientos generales de fuerza.
  - 6.12 Requerimientos de cableado de datos.
  - 6.13 Dimensionamiento físico del laboratorio.
  - 6.14 Ubicación de terminales para alumnos.
  - 6.15 Ejemplo de distribución de espacios.
  - 6.16 Resumen.

## Capítulo 7. Recomendaciones para la instalación de equipos dentro de los racks.

- 7.1 Introducción.
- 7.2 Distribución de equipos en racks.
- 7.3 Distribución de la potencia de fuerza en los racks.
- 7.4 Ejemplo de implementación.
- 7.5 Resumen.

## Capítulo 8. Cableado para la interconexión de equipo.

- 8.1 Introducción.
- 8.2 Cableado Intrarack.
- 8.3 Cableado Interrack.
- 8.4 Panel de parcheo RJ45.
- 8.5 Panel de parcheo V.35.
- 8.6 Panel de parcheo BNC.
- 8.7 Arreglo del cableado fijo dentro y fuera del rack.
- 8.8 Etiquetado
- 8.9 Elaboración del cableado
- 8.9.1 Cableado UTP.
- 8.9.2 Cableado V.35
- 8.9.3 Cableado coaxial BNC.
- 8.9.4 Etiquetado.
- 8.10 Ejemplo de implementación.
- 8.11 Resumen.

## Capítulo 9. Equipamiento del laboratorio.

- 9.1 Introducción.
- 9.2 Equipos de comunicaciones (DCEs.)
- 9.2.1 Enrutador.
- 9.2.2 Bridges.
- 9.2.3 Switch.
- 9.2.4 HUBs o concentradores.
- 9.2.5 Fraccionadores.
- 9.2.6 Metas técnicas y limitaciones de los dispositivos de red.
- 9.2.6.1 Escalabilidad.
- 9.2.6.2 Disponibilidad.
- 9.2.6.3 Desempeño de red.

- 
- 9.2.6.4 Seguridad
  - 9.2.6.5 Manejabilidad.
  - 9.2.6.6 Usabilidad.
  - 9.2.6.7 Adaptabilidad
  - 9.2.6.8 Costo – eficiencia (“Affordability”).)
  - 9.3 Equipos terminales (DTEs.)
  - 9.4 Terminales de acceso
  - 9.5 Servidor Web.
  - 9.6 Equipo y material didáctico.
  - 9.7 Equipamiento tentativo del laboratorio.
  - 9.8 Resumen.

## **Capítulo 10. Conexión local del laboratorio y conexión a Internet.**

- 10.1 Introducción.
- 10.2 Servicios más comunes sobre Internet.
- 10.3 Tipos de conexión
- 10.4 Esquema de conexión.
  - 10.4.1 Obtención de direcciones IP.
  - 10.4.2 Nombre del servidor en la red y registro del dominio o subdominio.
  - 10.4.3 Conexión del servidor Web a la red y seguridad del mismo.
  - 10.4.4 Acceso a los servicios brindados.
  - 10.4.5 Monitoreo de la actividad de la red y en el servidor.
- 10.5 Esquema de seguridad.
  - 10.5.1 Firewall.
  - 10.5.2 Servidor Proxy.
- 10.6 Posibles esquemas de conexión.
  - 10.6.1 Esquema 1. Esquema simple de conexión.
  - 10.6.2 Esquema 2: Firewall a nivel de red y dispositivo NAT
  - 10.6.3 Esquema 3. Servidor Proxy y enrutador NAT.
  - 10.6.4 Esquema 4. Esquema combinado.
- 10.7 Resumen.

## **Capítulo 11. Configuraciones y conexiones Tipo.**

- 11.1 Detalles técnicos de implementación.
- 11.2 Configuración lógica.
  - 11.2.1 Configuración del IOS.
  - 11.2.2 Configuración IP de un enrutador.
  - 11.2.3 Configuración de encapsulamiento en interfaces seriales.
    - 11.2.3.1 Encapsulación HDLC.
    - 11.2.3.2 Encapsulación PPP.
    - 11.2.3.3 Encapsulación Frame Relay.
  - 11.2.4 Mapeo de direcciones de hosts y tareas comunes.
  - 11.2.5 Configuración del enrutamiento estático.
  - 11.2.6 Configuración de enrutamiento por default.
  - 11.2.7 Configuración de listas de acceso para filtrar servicios no permitidos.
  - 11.2.8 Configuración NAT del enrutador.
- 11.3 Conexión física entre dispositivos.
  - 11.3.1 Conexión Ethernet en un enrutador.
  - 11.3.2 Conexión “back-to-back” entre enrutadores.
  - 11.3.3 Configuración de un Switch o HUB Cisco.

- 
- 11.4 Configuración de protocolos de enrutamiento.
  - 11.4.1 Configuración del protocolo de enrutamiento RIP.
  - 11.4.2 Configuración del protocolo de enrutamiento IGRP.
  - 11.4.3 Configuración del protocolo de enrutamiento EIGRP.
  - 11.4.4 Configuración del protocolo de enrutamiento OSPF.
  - 11.4.5 Verificación del funcionamiento y operación de los protocolos de enrutamiento.
  - 11.5 Resumen.

## Capítulo 12. Conexión a las consolas de equipos.

- 12.1 Introducción.
- 12.2 Líneas de terminal.
- 12.3 Acceso local.
- 12.3.1 Uso de Hyperterminal o de otros programas de emulación de terminal para conectarse a un equipo Cisco a través del puerto de consola.
- 12.4 Acceso remoto.
- 12.5 Esquema de conexión propuesto.
- 12.6 Resumen.

## Capítulo 13. Protocolos y tecnologías a soportar por el laboratorio.

- 13.1 Introducción.
- 13.2 Protocolos y tecnologías de capa 1 y 2 del modelo de referencia OSI.
- 13.3 Protocolos de capa 3 y 4 del modelo de referencia OSI.
- 13.4 Protocolos de enrutamiento IP.
- 13.5 Protocolos y servicios de capas superiores (4, 5 y 6) del modelo de referencia OSI.
- 13.6 Resumen.

## Capítulo 14. Ejemplos de prácticas sugeridas para el laboratorio.

- 14.1 Introducción.
- 14.2 Prácticas de ejemplo.
- 14.2.1 Protocolo de enrutamiento EIGRP.
- 14.3 Resumen.

## Capítulo 15. Administración del laboratorio.

- 15.1 Servicios del laboratorio.
- 15.2 Reglamento de uso en sitio y vía remota
- 15.3 Inventario de equipo
- 15.4 Conclusiones.

## Capítulo 16. Conclusiones generales.



---

## **DISEÑO E IMPLEMENTACIÓN DEL LABORATORIO DE DATOS DE LA FACULTAD DE INGENIERÍA.**

### **Objetivos.**

Esta tesis tal como su título lo indica, tiene como objetivo el realizar el diseño para la posterior implementación de un laboratorio de redes de datos para la facultad de ingeniería de la UNAM.

La idea surge de la necesidad de un espacio apropiado para la práctica de los conocimientos adquiridos en las clases de teoría de diversas materias impartidas por la Facultad de Ingeniería. En la actualidad no existe un laboratorio con dichas características y equipamiento necesario, a pesar de que las redes de datos han tenido un crecimiento muy rápido en los últimos años.

El área de las redes de datos es inmensa, debido a la cantidad de tecnologías, protocolos y estándares en uso durante muchos años, así como los que surgen continuamente. Entre ellas se pueden mencionar Ethernet, Token Ring, FDDI, IEEE 802.5, IEEE 802.3, CDDI, ATM, Frame Relay, TCP/IP, IPX, ISDN, PPP, protocolos de enrutamiento, listas de acceso, VLANs, VPNs, etc.

El conocimiento de estas tecnologías también implica la interoperabilidad entre ellas, por lo que la cantidad de variantes que se pueden tener en una red de datos es muy grande, es por esto que solo la práctica y la experimentación con equipos pueden mejorar y complementar la adquisición de los conocimientos aprendidos en la teoría

Los dispositivos requeridos para equipar a un laboratorio de redes de datos son diversos, además de que son costosos. La principal dificultad de implementación de un laboratorio como el que se desea, es contar con los recursos necesarios para poder equipar al mismo, es por ello que la idea de implementarlo surgió con la posibilidad de recibir equipos en donación que han sido retirados de operación pero que aun son útiles para la enseñanza.

### **Panorama general de la primera parte.**

En la primera parte de la tesis se establecen los conocimientos teóricos necesarios para poder entender las tecnologías y protocolos más usados, así como los medios de transmisión adecuados a las diferentes tecnologías que se estudien en esta tesis, de manera que se efectúa un análisis detallado de los temas que se tocan en esta parte.

El objetivo de esta parte de la tesis es que el lector tenga conocimiento previo suficiente para que pueda llevar a la práctica los conocimientos adquiridos en esta tesis.

Al final de esta tesis se encuentra un glosario donde se podrán consultar brevemente los términos mas usados a lo largo de la tesis.

---

## Capítulo 1.

### 1. Aspectos teóricos fundamentales para el entendimiento, uso y aplicación de las redes de datos.

#### 1.1 Principios y necesidades del uso de redes de datos

Uno de los grandes recursos del hombre para mejorar sus condiciones de vida ha sido el hecho de poder comunicarse con otros de su misma especie. Por lo tanto, el hombre siempre ha estado en busca de medios que le permitan tener formas más eficaces de comunicación, las cuales le permitan alcanzar diversos objetivos. El perfeccionamiento del lenguaje trajo como consecuencia un mayor entendimiento entre individuos, lo cual facilitó el flujo de conocimientos y de esta forma se aprovechó está cualidad para el desarrollo de la humanidad; que de no ser por esta evolución en la forma de comunicación del hombre, difícilmente se hubieran obtenido los avances que hasta el momento existen. A partir de entonces las formas de comunicarse entre seres humanos han ido adaptándose a las necesidades de desarrollo de la sociedad, y la comunicación ha sido y seguirá siendo un factor éxito para este punto.

Hoy en día las redes de computadoras facilitan la comunicación entre individuos ya sea de forma personal, dentro de una organización o entre organizaciones; permitiendo explotar información que puede llevarnos a mejorar nuestras condiciones de vida e incrementar la productividad empresarial. A esta era donde las computadoras y las redes de computadoras están jugando un papel muy importante en el desarrollo de la sociedad, se le ha denominado la "era de la informática", caracterizada por el uso de las computadoras como herramienta de uso diario.

#### 1.2 Definición

Una red de datos se puede definir como un conjunto de dispositivos interconectados entre sí, los cuales son capaces de compartir información digital y recursos tales como impresoras, archivos, servicios, etc. Otro de sus objetivos es hacer que todos los programas, datos (algún tipo de información digital, tales como bases de datos bancarios, acervos bibliográficos, correos electrónicos, etc.) y equipo estén disponibles para cualquier usuario de la red que así lo solicite, sin importar la localización física del mismo.

#### 1.3 Ventajas de usar redes de datos.

- **No importa la situación geográfica:** Hoy en día la mayoría de las organizaciones se encuentran ampliamente distribuidas de manera geográfica. Muchos de los departamentos requieren un flujo de información constante entre ellos, siendo la mejor opción cuando estos no se encuentran geográficamente cerca, una red de datos que les permita un fácil intercambio de información.
- **Compartir recursos e intercambio de información:** Las redes de computadoras permiten compartir recursos que son poco utilizados o que tienen un costo demasiado elevado para que cada usuario disponga de uno en particular (p. ej. impresora de alta calidad, grabadora de DVD, ect.). Al aumentar su grado de ocupación se amortiza rápidamente el costo de la adquisición del equipo. La utilización de redes permite el intercambio de datos entre los diferentes usuarios así como la capacidad de organización de los recursos lo cual tiene un impacto directo en la parte económica. Si los recursos con los que cuenta la red se pueden compartir esto tiene como consecuencia un ahorro significativo al usuario, además estos proporcionan mecanismos más sencillos para el intercambio de grandes volúmenes de información, sin necesidad de emplear dispositivos de almacenamiento externos como disquetes, cintas o CD-ROM.
- **Mayor efectividad y homogeneidad de las aplicaciones:** Cuando hay varios usuarios, cada uno tiende a utilizar aplicaciones que mejor se ajustan a sus necesidades y gustos. Esto puede provocar una situación de caos en la organización, por la gran variedad de formatos en los que se puede presentar la información y, lo que es peor, la falta de compatibilidad entre los mismos, que impediria



que un usuario leyera un archivo de un compañero. Estos problemas desaparecen si todos los usuarios usan los mismos programas.

Si además son aplicaciones que se comparten a través de la red, su instalación, gestión y mantenimiento son más efectivos.

#### 1.4 Una de las aplicaciones más exitosas de las redes de datos (El Internet).

El mejor ejemplo del éxito de las redes de datos es el Internet, el cual puede definirse como un conjunto de redes mundialmente interconectadas que permiten el libre paso de información entre ellas.

Sus orígenes se remontan al año 1969, como resultado de un proyecto militar (ARPANET), en el cual se interconectaron cuatro computadoras logrando una comunicación exitosa entre ellas. A partir de entonces ha experimentado una evolución constante y un crecimiento vertiginoso, convirtiéndose en un medio de difusión de información, colaboración, interacción y comercialización para cualquier individuo que tenga acceso a la misma, independientemente de su ubicación geográfica (ver figura 1.4.1).

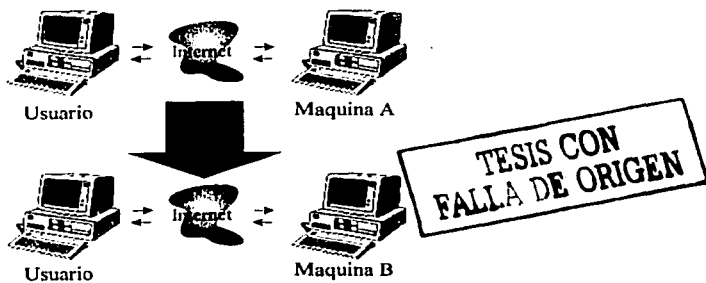


Figura 1.4.1. Conexiones por medio de Internet.

#### 1.5 Estandarización.

Conforme las primeras redes de datos fueron apareciendo, la interconexión entre ellas era sencilla mientras se trataba de los mismos fabricantes, pero imposible cuando se trataba de fabricantes distintos. La necesidad de interconectarse por parte de los dueños de esas redes, y la búsqueda de nuevos mercados por parte de los fabricantes, hizo que estos últimos hicieran acuerdos en cuanto a la fabricación de hardware y software y así lograr una comunicación exitosa entre sus equipos. Pero no todos los fabricantes accedían a modificar sus tecnologías (tales como IBM). Pronto fue evidente que era necesario el establecimiento organismos centrales que dirigiera el proceso de estandarización a nivel mundial para interfaces y protocolos de comunicación. Organismos como la ITU y la IEEE surgen con lo cual se comienza la estandarización de protocolos, haciendo posible la interconexión entre equipos de diferentes proveedores. Algunos de los organismos de estandarización más reconocidos se listan a continuación:

- International Organization for Standardization (ISO)
- American National Standards Institute (ANSI)
- Electronic Industries Association (EIA)
- Institute of Electrical and Electronic Engineers (IEEE)

- International Telecommunication Union Telecommunication Standardization Sector (ITU-T, antes CCITT)
- Internet Activities Board (IAB)

### 1.6 Modelo de referencia OSI.

Surgió de la necesidad de desarrollar una arquitectura de comunicaciones estándar que describe como la información en una computadora es transferida a una aplicación que reside en otra computadora. El modelo de referencia OSI es un modelo conceptual compuesto de 7 capas, cada una de ellas especificando funciones particulares, siendo cada capa razonablemente auto contenida, es decir que entre capas no existen funciones comunes. Además sirve como referencia a cualquier fabricante para adaptárselo, tanto a los distintos tipos de computadoras (diferentes marcas, con diferentes sistemas operativos, etc.) como a los tipos de medio de comunicación que se tengan que atravesar para acceder a éstos (redes de área local, redes telefónicas de conmutación, redes públicas de conmutación de paquetes, etc.).

La figura 1.6.1 muestra como el modelo de referencia OSI está estructurado en siete niveles o capas.

## ESTRATIFICACIÓN NIVELES OSI

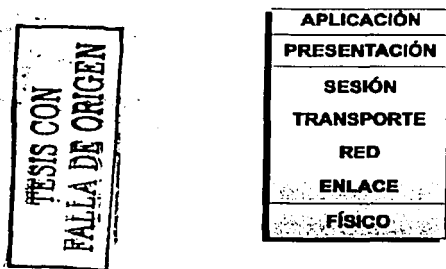
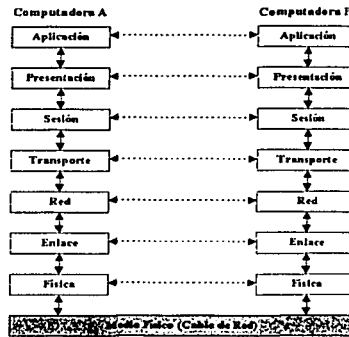


Figura 1.6.1. Niveles o capas del modelo de referencia OSI.

La comunicación que procede de una capa del modelo, generalmente se da con otras tres capas: la capa inmediata superior, la capa inmediata inferior y la capa análoga (o peer) en la computadora a la que se comunicará. La figura 1.6.2 muestra un ejemplo de comunicación entre capas:



**TESIS CON FALLA DE ORIGEN**

Figura 1.6.2. Comunicación entre capas

La comunicación entre capas de un mismo sistema se da en términos de los servicios que ofrece una capa a su capa inmediata superior, y de los servicios que obtendrá de la capa inmediata inferior. Los puntos de conexión entre capas son los denominados SAP's (Service Access Points). Por medio de ellos se intercambia información entre capas superiores n-1, donde n es el número de capa, también en ellos se distinguen los diferentes protocolos en la red, los números que los identifican son usualmente los mismos. Para hacer más seguros los sistemas y no se interfiera entre sí, los SAP's son registrados con la ISO.

Las 7 capas del modelo usan información de control para comunicarse con otras capas. Esta información de control toma las formas de encabezado o colas. El encabezado es información añadida al principio de los datos, mientras que las colas consisten en información añadida al final de los mismos datos que pasan de capas superiores a capas inferiores del modelo de referencia. La figura 1.6.3 muestra la adición de información de control entre capas:

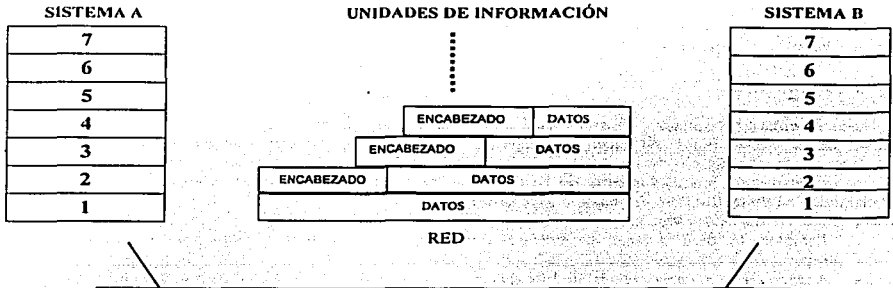


Figura 1.6.3 Adición de información de control entre capas.

El intercambio de información siempre es entre capas del mismo nivel.

---

### 1.6.1 Capa física.

La misión principal de esta capa es transmitir bits por un canal de comunicación, de manera que cuanto envíe el emisor llegue sin alteración al receptor.

La capa física proporciona sus servicios a la capa de enlace de datos, definiendo las especificaciones eléctricas, mecánicas, de procedimiento y funcionales para activar, mantener y desactivar el enlace físico entre sistemas finales, relacionando la agrupación de circuitos físicos a través de los cuales los bits son movidos.

La capa física no se apoya en los servicios de ningún otro nivel, y tampoco añade ninguna cabecera a la información proveniente del nivel anterior. Tiene cuatro tipos de características importantes:

- **Mecánicas.** Relacionadas con el tipo de conector que se utiliza.
- **Eléctricas.** Relacionadas con la forma de representación de los bits.
- **Funcionales.** Relacionadas con las funciones que van a desarrollar los circuitos individuales que hay entre el sistema y el medio físico.
- **Procedimentales.** Especifican la secuencia de eventos por la cual las cadenas de bits son transmitidas.

Los servicios que proporciona el nivel físico son los siguientes:

- Conexiones físicas.
- Puntos extremos de conexión física.
- Secuenciamiento.
- Notificación de condición de fallo.

Las funciones básicas que realiza son:

- Activación y desactivación de la conexión física, garantizar la conexión, pero no la fiabilidad de ésta.
- Transmisión de unidades de datos de servicio físico
- Gestión del nivel físico

### 1.6.2 Capa de enlace.

La capa de enlace proporciona sus servicios a la capa de red, suministrando un tránsito de datos confiable a través de un enlace físico. Al hacerlo, la capa de enlace de datos se ocupa del direccionamiento físico (comparado con el lógico), la topología de red, el acceso a la red, la notificación de errores, formación y entrega ordenada de tramas y control de flujo. Por lo tanto, su principal misión es convertir el medio de transmisión en un medio libre de cualquier tipo de errores.

Sus principales funciones son:

- Establece los medios necesarios para una comunicación confiable y eficiente entre dos máquinas en red.
- Agrega una secuencia especial de bits al principio y al final del flujo inicial de bits de la información, estructurando este flujo bajo un formato predefinido llamado trama. Suelen ser de unos cientos de bytes.

- Sincroniza el envío de las tramas, transfiriéndolas de una forma confiable libre de errores. Para detectar y controlar los errores se añaden bits de paridad, se usan CRC (Códigos Cíclicos Redundantes) y envío de acuses de recibo positivos y negativos, y para evitar tramas repetidas se usan números de secuencia en ellas.
- Controla la congestión de la red.
- Regula la velocidad de tráfico de datos.
- Controla el flujo de tramas mediante protocolos que prohíben que el remitente envíe tramas sin la autorización explícita del receptor, sincronizando así su emisión y recepción.
- Se encarga de la de secuencia, de enlace lógico y de acceso al medio (soportes físicos de la red).

El principal servicio del nivel de enlace es el de ofrecer una comunicación eficiente y fiable entre dos sistemas que estén directamente conectados.

### 1.6.3 Capa de red.

La capa de red proporciona sus servicios a la capa de transporte, siendo una capa compleja que proporciona conectividad y selección de ruta entre dos sistemas de hosts que pueden estar ubicados en redes geográficamente distintas. También se ocupa de aspectos de contabilidad de paquetes.

Es el responsable de las funciones de conmutación y enrutamiento de la información, proporcionando los procedimientos precisos necesarios para el intercambio de datos entre el origen y el destino, por lo que es necesario que conozca la topología de la red, con objeto de determinar la ruta más adecuada.

Podemos resumir las funciones de la capa de red en los siguientes puntos:

- Divide los mensajes de la capa de transporte en unidades más complejas, denominadas paquetes, y los ensambla al final.
- Debe conocer la topología de la subred y manejar el caso en que la fuente y el destino están en redes distintas.
- Se encarga de enrutar la información a través de la red, mirando las direcciones del paquete para determinar los métodos de conmutación y enrutamiento, y conmuta los paquetes de la fuente al destino a través de enrutadores intermedios.
- Envía los paquetes de nodo a nodo usando ya sea un circuito virtual o como datagramas.
- Controlar la congestión de la subred.

En esta capa es donde trabajan los enrutadores.

### 1.6.4 Capa de transporte.

Este nivel asegura que las unidades de datos sean entregadas sin errores, en secuencia y sin duplicaciones ni pérdidas.

También está relacionada con la optimización del uso de los servicios de red y el ofrecimiento de servicios de control de ciertos parámetros de la comunicación.

Las funciones típicas del nivel del transporte son la segmentación y la multiplexación. La multiplexación consiste en mandar los paquetes de varias entidades de nivel  $n$  a través de una única entidad de nivel  $n-1$  para que de esta manera haya un mejor aprovechamiento de la comunicación.

Por tanto, la función básica del nivel de transporte es recibir datos del nivel de sesión, fragmentarlos en unidades más pequeñas si es necesario, y pasar éstas al nivel siguiente, garantizando que todos los fragmentos lleguen correctamente al otro extremo, todo ello de la manera más eficiente posible y reensamblar los fragmentos en el otro extremo.

El nivel de transporte puede ofrecer el servicio de detección y corrección de errores, de manera que se puede proporcionar una conexión de transporte como un canal punto a punto (virtual) libre de errores.

---

Las funciones que puede desempeñar el nivel de transporte son las siguientes:

- Establecimiento y liberación de conexiones de transporte.
- Transferencia de datos por la conexión de transporte, incluyendo las funciones de secuenciamiento, bloqueo, segmentación, multiplexación, control de flujo, detección y recuperación de errores e identificación de la conexión de transporte.

#### 1.6.5 Capa de sesión.

Este nivel recoge una serie de mecanismos que permiten controlar y coordinar el flujo de datos entre procesos de aplicación.

Estos servicios se podrían implementar directamente en las aplicaciones, pero al estar tan extendido su uso se decidió implementarlos en este nivel. Ejemplos de servicios ofrecidos por este nivel son el control del diálogo, donde se puede especificar que el diálogo sea simultáneo (si las dos aplicaciones intercambian datos simultáneamente) o alternado (sólo transmite datos una a la vez).

Otro servicio que presta esta capa es el mecanismo de Checkpoint, que consiste en ir marcando ciertas partes de un mensaje para que, en el caso de que se interrumpiera la comunicación, la retransmisión se realizase a partir de estos puntos, sin tener que retransmitir el mensaje completo con el consiguiente ahorro de tiempo.

Además, este nivel proporciona los medios necesarios para la cooperación de las entidades de presentación, para organizar y sincronizar su diálogo, y para gestionar su intercambio de datos. Para ello, el nivel de sesión proporciona los servicios para establecer una sesión cada vez que se desee establecer una comunicación entre entidades de presentación.

Dentro de las funciones que debe realizar el nivel de sesión se podría destacar las siguientes:

- Transferencia de datos.
- Recuperación de la conexión de sesión.
- Gestión del nivel de sesión.

#### 1.6.6 Capa de presentación.

El nivel de presentación está relacionado con la sintaxis de los datos intercambiados entre dos entidades de aplicación.

Su propósito es resolver las diferencias en el formato y la representación de los datos, y, para ello, se define una *sintaxis estándar que sea transformable en cualquier sintaxis específica de cualquier entidad de aplicación*. Por tanto, este nivel es el que garantiza el carácter abierto del modelo OSI, ya que se encarga de las funciones de interpretación y presentación de la estructura de la información recibida.

Un ejemplo de esta posible diferencia de representación de los datos en dos computadoras distintas, es que cada una de ellas utilice un código de representación diferente (por ejemplo, una usa el código ASCII y otra usa el código EBCDIC).

Las funciones que corresponden este nivel son las siguientes:

- Traducir entre varios formatos de datos utilizando un formato común, estableciendo la sintaxis de la información transmitida. Para ello convierte los datos desde el formato local al estándar de red y viceversa.

- Definir la estructura de los datos a transmitir. Por ejemplo, en el caso de un acceso a base de datos, así como el orden de transmisión y la estructura de los registros.
- Definir el código a usar para representar una cadena de caracteres (ASCII, EBCDIC, etc).
- Dar formato a la información para visualizarla o imprimirla.
- Comprimir los datos si es necesario.
- Aplicar a los datos procesos criptográficos.

### 1.6.7 Capa de aplicación.

El nivel de aplicación se encarga de la semántica (el significado de la información intercambiada), es la capa del modelo OSI más cercana al usuario, y está relacionada con las funciones de mas alto nivel que proporcionan soporte a las aplicaciones o actividades del sistema, suministrando servicios de red a las aplicaciones del usuario y definiendo los protocolos usados por las aplicaciones individuales. Es el medio por el cual los procesos de aplicación de usuario acceden al entorno OSI.

Su función principal es proporcionar los procedimientos precisos que permitan a los usuarios ejecutar los comandos relativos a sus propias aplicaciones.

Los procesos de las aplicaciones se comunican entre sí por medio de las entidades de aplicación asociadas, estando éstas controladas por protocolos de aplicación, y utilizando los servicios del nivel de presentación.

Difiere de las demás capas debido a que no proporciona servicios a ninguna otra capa OSI, sino solamente a aplicaciones que se encuentran fuera del modelo OSI. La capa de aplicación establece la disponibilidad de los diversos elementos que deben participar en la comunicación, sincroniza las aplicaciones que cooperan entre sí y establece acuerdos sobre los procedimientos de recuperación de errores y control de la integridad de los datos.

Algunos ejemplos de procesos de aplicación son:

- Programas de hojas de cálculo.
- Programas de procesamiento de texto.
- Transferencia de archivos (ftp).
- Login remoto (rlogin, telnet).
- Correo electrónico (mail – smtp).
- Páginas Web.

**TESIS CON FALLA DE ORIGEN**

### 1.7 Estructura de un sistema de Comunicaciones de datos.

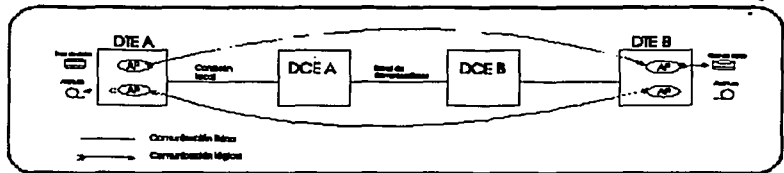


Figura 1.7.1 Estructura de un sistema de comunicación de datos básico.

En la figura 1.7.1 se muestra un sistema de comunicaciones de datos muy sencillo. El proceso de aplicación (AP) es la aplicación final del usuario y consiste usualmente en un programa de computadora. Ejemplos típicos son bases de datos, algún sistema de reservación o de consulta, etc.

Se puede observar también como el sitio A puede ejecutar un programa y acceder a un proceso de aplicación en el sitio B; de manera similar, un proceso de aplicación que reside en el sitio B accesa a proceso de aplicación en el sitio A.

La aplicación reside en las máquinas del usuario final que de manera genérica son denominadas data terminal equipment o DTE (equipo terminal de datos). Los DTEs pueden ser tan grandes y complejos como un Main Frame de IBM o tan sencillos como una terminal o PC.

La función de una red de comunicaciones es interconectar DTEs, de tal forma que estos puedan comunicarse entre sí, permitiéndoles compartir recursos. Los dispositivos cuya función es precisamente conectar DTEs a la línea de comunicación son los llamados circuit-terminating equipment o DCE's.

En la figura 1.7.2 se muestra un sistema de comunicaciones usando enrutadores como DCE's y en la figura 1.7.3 usando switches.

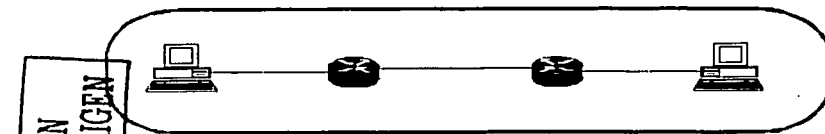


Figura 1.7.2. Sistema de comunicaciones usando enrutadores.



Figura 1.7.3. Sistema de comunicaciones usando switches.

## 1.8 Topologías de red.

Se define topología de una red a la forma en la que se distribuyen las estaciones de trabajo y las conexiones a la red.

Para cada red de área local se deben definir dos tipos de topologías: la topología lógica y la topología física. Aunque en un primer momento pudiera parecer difícil distinguir un tipo de topología del otro, con el término físico identificamos la disposición de las conexiones físicas a la red, esto es, los criterios que se siguen para conformar la estructura de la red, mientras que con el término lógico se pretende resaltar el comportamiento que tendrán las estaciones al comunicarse.

Se desglosará a continuación cada una de ellas:



a) **Topología lógica.** Define cómo se distribuyen los datos entre las estaciones de trabajo o computadoras que componen la red.

- **Topología lógica en bus.** Los datos se difunden sin ningún orden preestablecido, es decir, cualquier estación puede capturar los mensajes del medio de transmisión.
- **Topología lógica en anillo.** Los datos se difunden con un orden preestablecido, por ejemplo, A, B, C, etc., es decir, si una estación A transmite un mensaje, éste pasa a B, independientemente de si va dirigido a la estación B o a otra, luego por C, etc. El mensaje continúa su recorrido en orden, hasta alcanzar a la estación destino.

b) **Topología física.** Las estaciones de trabajo de una red se comunican entre sí mediante una conexión física, y el objeto de la topología es buscar la forma más económica y eficaz de conectarlas para, al mismo tiempo, facilitar la fiabilidad del sistema, evitar los tiempos de espera en la transmisión de los datos, permitir de manera eficiente el aumento de estaciones dentro de la red, etc. Las distintas opciones a la hora de determinar la topología son:

- **Topología de física de Bus.**

En la figura 1.8.1 se muestra como todos los dispositivos se encuentran conectados a un medio de transmisión de manera plana, es decir que la transmisión de uno es escuchada por todos al mismo tiempo. Cada estación recogerá únicamente la información que específicamente esté dirigida a ella.

El canal se comporta como un elemento pasivo, por lo que las señales se propagan bidireccionalmente. En los extremos del bus se colocan resistencias de terminación (RT) que absorben la señal. Cada estación se inserta en la red mediante un TAP, que incluye un transceiver (transmisor y receptor).

Los TAP producen pequeñas reflexiones de la señal, por lo que conviene predeterminar su posición en el bus, de forma que estas reflexiones no acaben sumándose y destruyendo la señal. La distancia total del bus está limitada debido a la atenuación total de la señal en el medio de transmisión, ya que la señal de cada estación debe llegar a todas las demás. El inconveniente de esta topología es el control de acceso al medio, ya que, aunque varias estaciones intenten transmitir a la vez, al existir un único medio de transmisión, sólo una de ellas puede hacerlo, por lo que se deberán de establecer de los adecuados mecanismos que permitan la comunicación. Además, resulta complicado determinar los puntos en los que se producen problemas de cableado, ya que todas las estaciones utilizan el mismo medio.

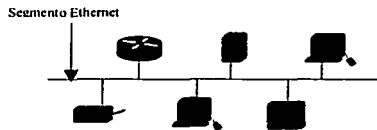


Figura 1.8.1. Todos los dispositivos se encuentran conectados a un mismo medio.

- **Topología física de Anillo.**

En la figura 1.8.2.1 se muestra como están conectados los dispositivos uno tras otro en cadena formando un anillo. Si un dispositivo quiere transmitir información a otro no directamente conectado, los dispositivos

TESIS CON FALLA DE ORIGEN

intermedios tendrán que retransmitir la información generada por el primer dispositivo hasta que llegar a su destino final.

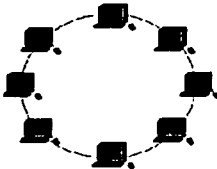


Figura 1.8.2 Conexión de dispositivos en forma de anillo.

- Topología física jerárquica o árbol.

En la figura 1.8.3.1 se muestra como en esta topología varios dispositivos son concentrados en otro para su comunicación, que a la vez puede estar concentrado en otro dispositivo de mayor jerarquía para su comunicación.

TESIS CON FALLA DE ORIGEN

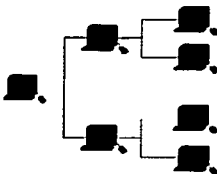
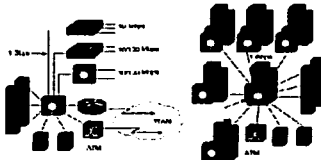


Figura 1.8.3. Dispositivos conectados en forma jerárquica.

- Topología física de estrella.

En las figuras 1.8.4 y 1.8.5 se muestra como el tipo de topología física más común, y consiste en un dispositivo central al cual se conectan todos los demás dispositivos para su comunicación. Esto es un factor que repercute negativamente, cuando se pretende utilizar esta topología para sistemas con un número elevado de estaciones, ya que al agruparse todas las conexiones en un único dispositivo central, la gestión se convierte en una tarea crítica, propensa a errores.



Dadas las características de la topología, las comunicaciones entre las estaciones y el elemento de conexión central son muy rápidas; en cambio, introduce un retardo a considerar en la comunicación entre estaciones de trabajo.

Figuras 1.8.4 y 1.8.5 Dispositivos centrales a los cuales se conectan los demás dispositivos

- **Topología de malla.**

En la figura 1.8.6 se muestra una topología de uso común en redes WAN, consiste en la conexión entre dispositivos de acuerdo al interés de tráfico y de redundancia en conectividad.

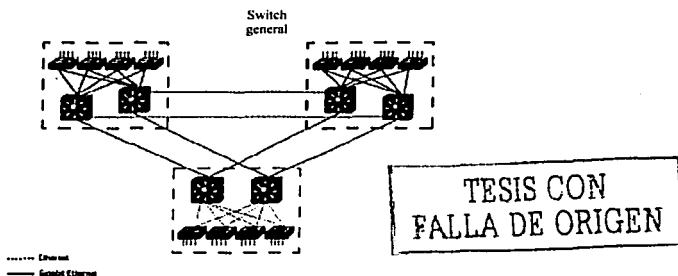


Figura 1.8.6 Conexión de dispositivos de acuerdo al interés y redundancia en el enlace

## 1.9 Resumen.

En este capítulo se listaron las ventajas que proporciona el uso de una red de datos, así como su definición de la misma, además de el surgimiento de llevar a cabo una estandarización de los diferentes dispositivos existentes en el mercado, en pocas palabras que fueran compatibles los productos de los diferentes fabricantes entre sí y por otro lado las diferentes arquitecturas de comunicación que cada fabricante utilizaba, debido a esto surge la necesidad de crear un modelo de comunicaciones estándar denominado como el modelo de referencia OSI y sus diferentes niveles o capas que cumplen con diversas tareas para llevar a cabo la comunicación entre los sistemas.

Por otra parte se muestra la estructura básica de un sistema de comunicaciones de datos, así como los dispositivos por los que se conforma el mismo.

Por último se muestran las diferentes topologías con las cuales los diferentes dispositivos de la red se pueden interconectar, claro que esto depende de las necesidades de la conexión, así como el tipo de servicios o tráfico que circularan por la red.

## Capítulo 2. Medios de transmisión.

### 2.1 Introducción.

El medio de transmisión es una parte fundamental para el diseño de la red ya que este puede limitar la velocidad de intercambio de información y, además, es un aspecto que tiene importancia a la hora de realizar la implementación física de la misma. En seguida se detallan las características más significativas de los diferentes medios de transmisión, así como sus usos más comunes en el área de las redes de datos.

### 2.2 Cable coaxial.

El cable coaxial está formado por un conductor de cobre en su parte central, denominado núcleo; un material aislante separa el interior de un segunda capa conductora, que puede aparecer como una malla, o también un cilindro, de cobre. La malla está usualmente conectada a un sistema de tierras, y su función principal es minimizar la interferencia eléctrica y de radiofrecuencia.

La utilización de cable coaxial conduce a una buena combinación de ancho de banda elevado y adecuada inmunidad al ruido. El ancho de banda que se puede obtener depende de la longitud del cable; para cables de 1 km, por ejemplo, es posible conseguir velocidades de datos de hasta 10 Mbps. Los cables coaxiales se emplean ampliamente en redes de área local y para transmisiones de larga distancia, en el sistema telefónico.

El cable coaxial fue inventado en 1929 y usado comercialmente desde 1941(ver figura 2.2.1).

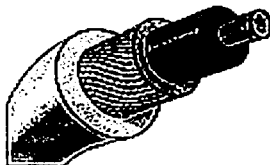
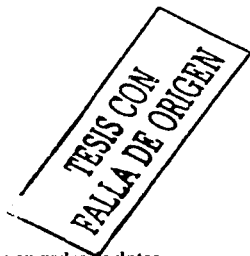


Figura 2.2.1. Cable coaxial

Uso en redes de datos.

#### 2.2.1 Ethernet.

El cable coaxial es usado como medio de transmisión en dos implementaciones físicas de Ethernet 802.3 : 10base2 y 10base5.

**10base2:** Utiliza para su implementación cable coaxial denominado "thin" (delgado) de 50 ohms de impedancia nominal, utilizado únicamente para transmisión digital (RG-58 A/U) con una longitud mínima de 0.5 metros y máxima de 185 metros entre dispositivos. Los cables en este tipo de implementación usan conectores del tipo BNC. La tarjeta de red del dispositivo a conectar a la red necesita de un conector tipo "T", que es un conector que une ambas partes del cable proporcionando una tercera conexión para la computadora. En uno de los extremos del conector "T" se conecta un terminador a 50 ohms (ver figuras 2.2.1.1 y 2.2.1.2)

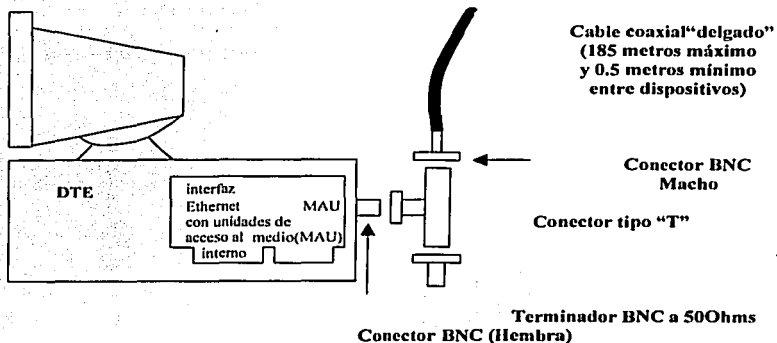


Figura 2.2.1.1. Tipo de conexión 10base2

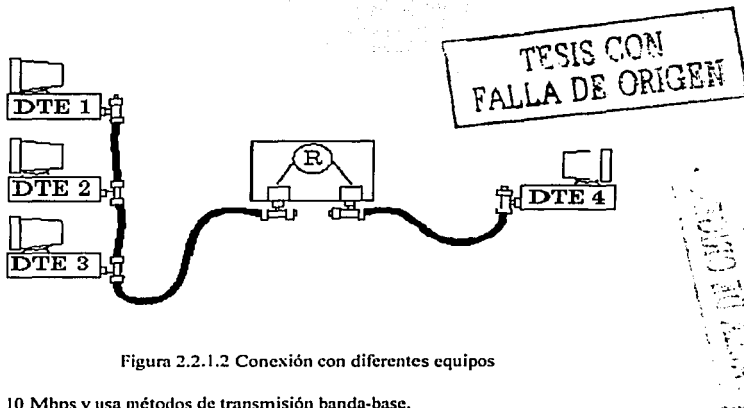


Figura 2.2.1.2 Conexión con diferentes equipos

10base2 opera a 10 Mbps y usa métodos de transmisión banda-base.

**10base5:** Utiliza para su implementación cable coaxial "Thick" (grueso) con una impedancia nominal de 50 ohms; con una longitud máxima de 500 metros. El cable usado es prácticamente inflexible. Esta fue la primera implementación física de Ethernet.

En esta implementación la interfaz Ethernet del dispositivo es conectada al cable coaxial mediante un MAU (Media Attachment Unit o unidad de acceso al medio), el cual provee la conexión eléctrica y conversión de

señales entre la interfaz Ethernet y el segmento de red. El MAU esta equipado con un conector macho AUI de 15 pines, y es alimentado por la interfaz Ethernet (ver figuras 2.2.1.3 y 2.2.1.4).

Un cable AUI es utilizado para proveer la conexión entre un MAU y una interfaz Ethernet.

10base5 opera a 10 Mbps y usa métodos de transmisión banda-base.

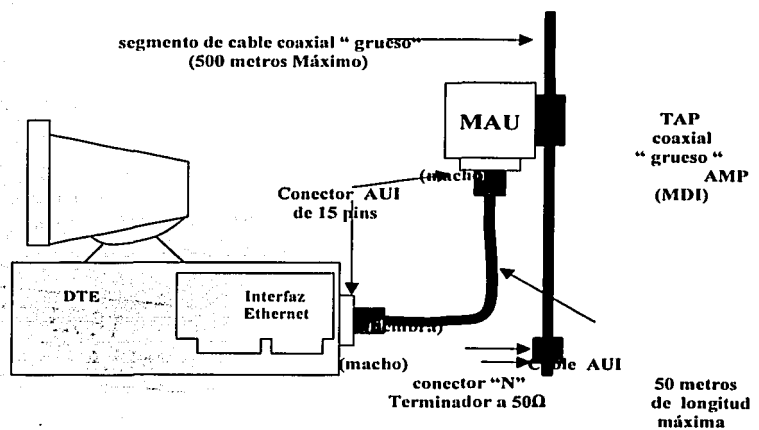


Figura 2.2.1.3. Tipo de conexión 10base5

TESIS COI.  
FALLA DE ORIGEN.

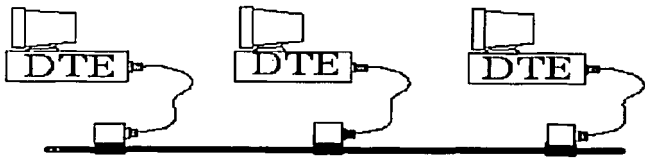


Figura 2.2.1.4. Conexión con diferentes equipos

2.2.2 Cable Modem.

El "Cable Modem" es un dispositivo que permite el acceso a alta velocidad a Internet, así mismo, brinda servicios de transporte de datos, empleando para ello la red de televisión por cable.

La mayoría de los Cable Modems son dispositivos externos que se conectan por un lado a la red de televisión por cable, mientras que por el otro se conectan a la PC del usuario.

Aprovechando la infraestructura física de las compañías de televisión por cable, la transmisión de datos por cable coaxial se ha vuelto una opción más de conectividad al Internet.

Los dispositivos a conectarse usan cable módems, usando las especificaciones de interfase sobre tipo de cable. Los estándares de este cable proveen las bases para comunicar cualesquiera dos equipos terminales equipados con cable módems, los cuales están diseñados para operar sobre canales específicos de cable.



Figura 2.2.2.1. Dispositivo Cable Modem.

### 2.2.3 G.703.

Una de las implementaciones físicas para la transmisión del primer orden de PDH (2,048 kbps) es el uso de cable coaxial de 75 ohms. Usando como terminadores conectores BNC.

### 2.2.4 G.753.

Una de las implementaciones físicas para la transmisión del tercer orden de PDH (34,368 Kbps) es el uso de cable coaxial de 75 ohms. Usando como terminadores conectores BNC.

## 2.3 Par trenzado.

El par trenzado está constituido por unos conductores de cobre trenzado y aislados entre sí, los cuales se han enroscado en pares para reducir la inducción electromagnética. Cada alambre tiene su propio aislante. Dado que es común el requerimiento de más de un par trenzado para comunicar dispositivos, es usual que muchos pares sean colocados dentro de un mismo cable (ver figura 2.3.1).

### Cable de Par Trenzado (Dos Hilos)

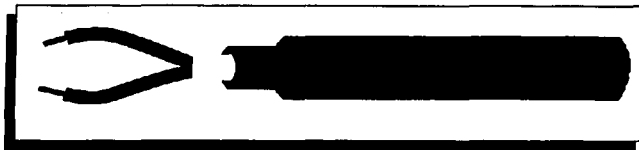


Figura 2.3.1 Cable par trenzado.

A continuación se muestran las dos implementaciones más comunes para este medio de transmisión:

a) **Par trenzado no apantallado o UTP ("unshielded twisted pair")** : compuesto por cuatro pares de hilos, trenzados par a par, y revestidos de un aislante plástico de colores para la identificación de los pares. Cada par de hilos se encuentra aislado de los demás. Es el normal y más usado en todas las redes locales por ser el más barato. El número de pares por cable son 4, 25, 50, 100, 200 y 300. Cuando el número de pares es superior a 4 se habla de cables multipar. (Si se habla de 4 pares quiere decir que en total hay 8 cables) el trenzado del cable se utiliza para reducir las interferencias.

Existen diferentes categorías:

- UTP1: transmite Voz.
- UTP2: transmite a 4 Mbps.
- UTP3: transmite de 10 Mbps.
- UTP4: transmite de 20 Mbps.
- UTP5: transmite a 100 Mbps.

El cable no apantallado o UTP tiene una impedancia de 100 Ohms.

Al ser de unos 0.52 mm de grosor, de poco peso y gran flexibilidad se convierte en un cable de fácil manejo e instalación, no requiriendo grandes canalizaciones en su trazado.

b) **Par trenzado apantallado (STP)**: formado por una capa exterior plástica aislante y una capa interior de papel metálico, dentro de la cual se sitúan normalmente cuatro pares de cables, trenzados par a par, con revestimientos plásticos de diferentes colores para su identificación. Combina las técnicas de blindaje, cancelación y trenzado de cables. El cable STP proporciona resistencia contra la interferencia electromagnética y de la radiofrecuencia sin aumentar significativamente el peso o tamaño del cable. El cable de par trenzado apantallado tiene las mismas ventajas y desventajas que el cable de par trenzado no apantallado. STP brinda mayor protección contra todos los tipos de interferencia externa, pero es más caro que el cable de par trenzado no blindado. El cable apantallado tiene una impedancia de 150 Ohms.

Uso en redes de datos

### 2.3.1 Ethernet

El par trenzado es usado en las siguientes implementaciones físicas de Ethernet: 10baseT, 100baseT, 100baseT4.

**10baseT**: Opera a 10 Mbps usando cable UTP. La distancia entre dispositivos no debe ser mayor a 100 metros, todos ellos conectados un repetidor central, que puede ser un Hub o un Switch (ver figura 2.3.1.1).

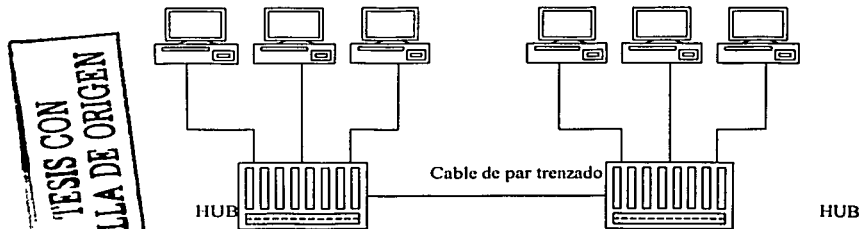


Figura 2.3.1.1 Conexiones con cable de par trenzado



Especificaciones para 10baseT:

Tipo de cable: UTP con dos pares trenzados de 22, 24 o 26 AWG.

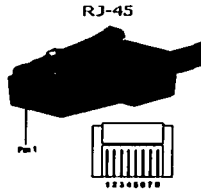
Vueltas por pie: 2 o 3(min.)

Impedancia Nominal: 100 ohms

Longitud máxima del cable: (100m)

Máxima tasa de transmisión: 10 Mbps

Los conectores usados son RJ-45 y se muestran en la figura 2.3.1.2



TESIS CON  
FALLA DE ORIGEN

Figura 2.3.1.2. Conector RJ-45

**100baseT:** Implementación física de Ethernet que usa cable UTP o STP categoría 5 y que opera a 100 Mbps. Usa la misma configuración física que 10baseT.

**100baseT4:** Implementación de Ethernet que usa cable UTP categoría 3 y que opera a 100 Mbps. A diferencia de 100baseT, 100baseT4 usa 4 pares trenzados para la transmisión de datos. Usa la misma configuración física que 10baseT.

Las longitudes máximas dependen del tipo de cable y la velocidad de operación.

### 2.3.2 xDSL y DS0's.

Estas tecnologías utilizan el par trenzado telefónico para la transmisión de información digital. xDSL puede manejar hasta 2,048 Mbps, mientras que el DS0 varía de entre 64 y 128 Kbps

### 2.4 Fibra óptica.

Los desarrollos en el campo de la tecnología óptica han hecho posible la transmisión de información mediante pulsos de luz. Un pulso de luz puede utilizarse para indicar un bit de valor 1; la ausencia de pulso luminoso indicará la existencia de bit de valor 0. Dada la alta frecuencia de la luz visible, el ancho de banda de un sistema de transmisión óptica presenta un potencial enorme.

Un sistema de transmisión óptica tiene tres componentes: el medio de transmisión, la fuente de luz y el detector. El medio de transmisión es una fibra ultradelgada de vidrio o silicio fundido. La fuente de luz puede ser un diodo emisor de luz (LED) o un diodo láser; cualquiera de los dos emite pulsos de luz cuando se les aplica una corriente eléctrica. El detector es un fotodiodo que genera una señal eléctrica en el momento en el que recibe un pulso de luz. Al colocar un LED o un diodo láser en el extremo de una fibra óptica, y un fotodiodo en el otro, se tiene un sistema de transmisión de datos unidireccional que acepta una señal eléctrica, la convierte y la transmite por medio de pulsos de luz y después reconvierte la salida en una señal eléctrica, en el extremo receptor.

Este cable está constituido por uno o más hilos de fibra de vidrio silicio fundido (ver figura 2.3.1).



### Agrupación Múltiple de Fibras Ópticas

Figura 2.4.1. Fibra óptica

Cada fibra consta de:

- Un núcleo central de fibra con un alto índice de refracción.
- Una cubierta que rodea al núcleo, de material similar, con un índice de refracción ligeramente menor.
- Una envoltura que aísla las fibras y evita que se produzcan interferencias entre fibras adyacentes, a la vez que proporciona protección al núcleo. Cada una de ellas está rodeada por un revestimiento y reforzada para proteger a la fibra.

Existen dos clases de fibra óptica:

a) **Monomodo:** Dan un gran ancho de banda debido a que están fabricadas de un material y con unas dimensiones tales que sólo puede tener un solo modo de propagación, esto permite que se tenga gran alcance y por lo tanto resulten óptimas para redes extensas. Pero dada su complejidad en su elaboración son más caras y necesitan aparatos caros de apoyo.

b) **Multimodo:** Se transmiten varios modos electromagnéticos por la fibra, denominándose por este motivo fibra multimodo. En este último caso, debido a las diferentes velocidades de propagación, los modos no llegan a su destino al mismo tiempo y se produce un efecto negativo que se conoce con el nombre de *dispersión modal* (el efecto de la dispersión modal sobre un pulso cuadrado es su suavizado y ensanchamiento) esta sería la mayor desventaja de este tipo de fibra aunque por otro lado es más barata que la fibra monomodo.(ver figura 2.4.2)

### Fibra óptica

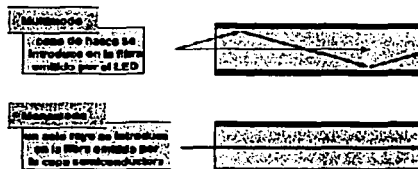


Figura 2.4.2. Modos de propagación en la fibra óptica

## Uso en redes de datos.

### 2.4.1 Ethernet

La fibra óptica se usa en las siguientes implementaciones físicas de Ethernet: 100baseFX y 1000baseFX.

100baseFX: Opera a 100Mbps usando fibra óptica multimodo, y permite una distancia máxima de 42 metros por cable. Esta implementación usa dos hilos de fibra por cable, uno para transmisión y otro para recepción(ver figura 2.4.1.1). Los conectores usados son del tipo SC, ST o MIC(ver figura 2.4.1.2).

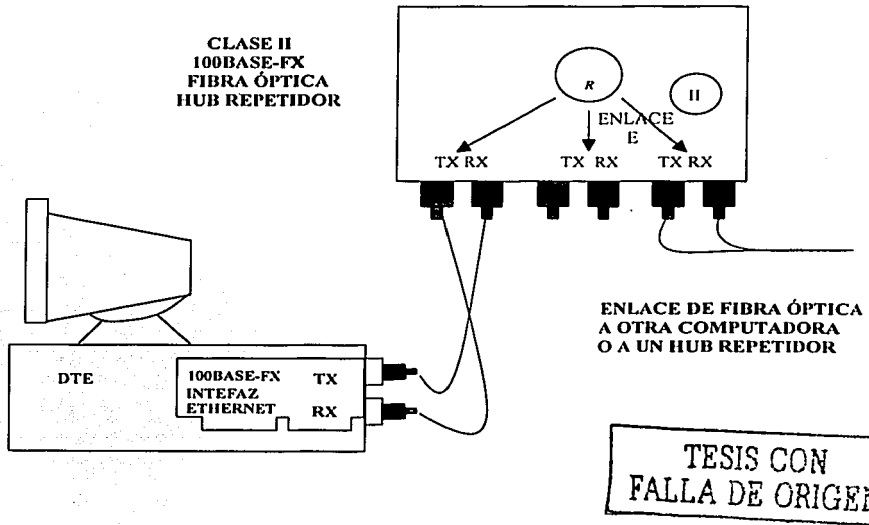


Figura 2.4.1.1 Tipo de conexión 100baseFX.

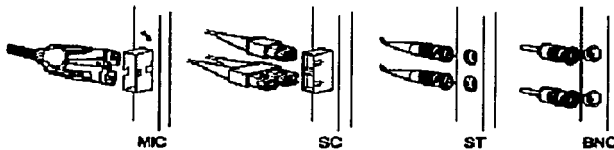
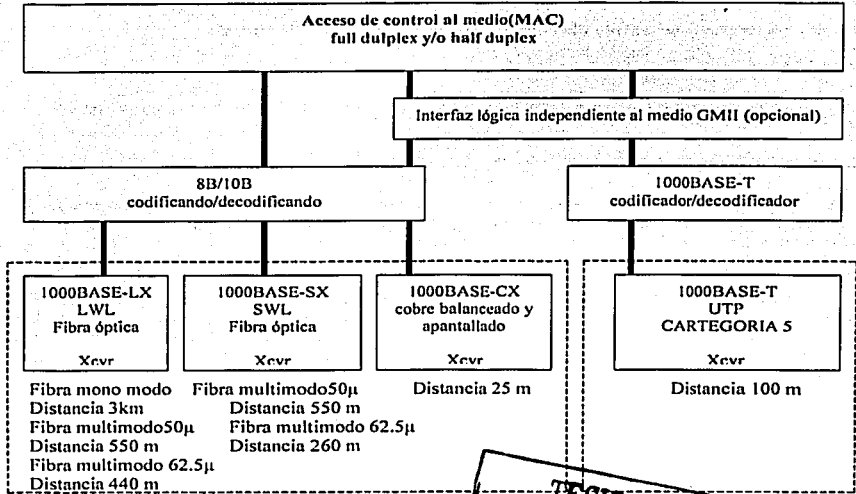


Figura 2.4.1.2. Tipos de conectores

---

**1000baseSX, 1000baseLX. Implementaciones físicas de Ethernet a 1 Gbps que usan fibra óptica. En la implementación SX se pueden tener distancias de hasta 440 metros, mientras que en LX las distancias pueden ser de hasta 3 kilómetros.**

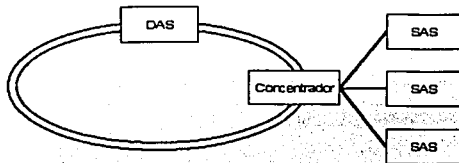
## CAPAS SUPERIORES DE ETHERNET



TESIS CON FALLA DE ORIGEN

### 2.4.2 FDDI.

FDDI usa fibra óptica como principal medio de transmisión, permitiendo distancias de 2 kms usando fibra multimodo y de distancias aún mayores usando fibras monomodo, los tipos de conectores usados son MIC. FDDI utiliza dos fibras, las cuales transmiten información en sentidos opuestos formando dos anillos. En operación normal, sólo un anillo es usado para la transmisión de información a 100Mbps, quedando el otro como respaldo en caso de alguna falla. Los dispositivos llamados "Dual Station Attachment" o DAS, tienen conexión a ambos anillos y son capaces de conectar ambos anillos para dar continuidad a la conectividad de las estaciones en caso de falla de alguna fibra o dispositivo. Los dispositivos "Single Attachment Station" o SAS son concentrados por un "Dual Attachment Concentrator" o DAC (concentrador) para su conexión al anillo principal (ver figura 2.4.2.3).



### Figura 2.4.1.3 Conexión FDDI

#### 2.4.3 SDH

Tecnología de transmisión que usa fibra óptica entre la mayoría de sus dispositivos.

#### 2.4.4 ATM

ATM usa como medio de transmisión principal a SDH, por lo que las interfaces hacia este son con fibras ópticas.

#### 2.5 Espacio Libre

Se basan en la transmisión de ondas electromagnéticas, que pueden recorrer el vacío del espacio exterior y medios como el aire, por lo que no es necesario un medio físico para las señales inalámbricas, lo que hace que sean un medio muy versátil para el desarrollo de redes.

La aplicación más común de las comunicaciones de datos inalámbricas es la que corresponde a los usuarios móviles.

Algunos fabricantes ya están ofreciendo redes de área local sin cables utilizando esta tecnología o rayos infrarrojos. Estas tecnologías están siendo de gran aceptación, pues en las oficinas el cableado es uno de los aspectos negativos de las LAN's. Sin embargo, actualmente se utilizan más en redes de área metropolitana y de área extensa para interconectar redes de área local y con esto se da comienzo a la era de lo inalámbrico (ver Figura 2.5.1).

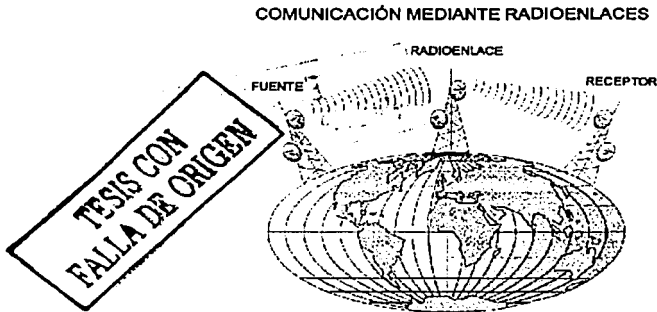


Figura 2.5.1 Enlace de comunicaciones inalámbrico

#### 2.6 Resumen.

En este capítulo se mostraron los diferentes medios de transmisión que pueden ser empleados en la implementación de una red de datos, así como sus alcances y limitaciones de los mismos. También se presentaron aplicaciones de los medios de transmisión en diferentes tecnologías que serán más profundamente analizadas en el siguiente capítulo.

RECEIVED  
MEDICAL DEPARTMENT

## Capítulo 3. Tecnologías LAN.

# TESIS FALLA DE ORIGEN

### 3.1 Introducción.

Una Red de Área Local es un sistema de comunicación que cubre una área geográfica limitada (por ejemplo: la red en un edificio o de un grupo de edificios dentro de un cierto intervalo de distancia la cual puede variar de acuerdo al tipo de tecnología en uso), la cual interconecta dispositivos que aportan diferentes funciones a la Red, así como la comunicación entre ellos.

Los dispositivos o recursos que se interconectan entre sí pueden ser los siguientes:

- Estaciones de trabajo.
- Impresoras.
- Dispositivos de Almacenamiento.
- Enrutadores.
- Hubs.

Las redes de área local «Local Area Network» (LAN); constituyen el ámbito de mayor crecimiento en la actual industria de productos informáticos. La principal razón de este crecimiento es que constituyen el medio más adecuado para la automatización de oficinas.

En las empresas y organizaciones, una red de área local facilita la conectividad entre máquinas informáticas heterogéneas y, por otra parte, contribuye a homogeneizar el entorno informático. De esta forma, se puede acceder desde máquinas remotas muy diversas a los mismos datos de los que dispondría la computadora que posee localmente la información.

Bajo el punto de vista de la IEEE y de acuerdo a las normas de estandarización se podrá tener un mayor entendimiento de los mecanismos de transmisión de las diferentes tecnologías existentes para la implementación de una red LAN, se explicará con mayor detalle el funcionamiento de la capa de enlace que se encuentra dividida en dos partes: en la parte inferior se encuentra la subcapa MAC (Media Access Control) responsable de las técnicas de acceso al medio de transmisión y el direccionamiento físico de dispositivos; mientras que en la parte superior se encuentra el estándar IEEE 802.2 ó LLC (Logical Link Control) que define las funciones lógicas de la capa de enlace así como la disponibilidad de SAP (Service Address Point) para la adecuada transmisión o recepción de información a protocolos que operan en capas superiores del modelo de referencia OSI (ver la figura 3.1.1).

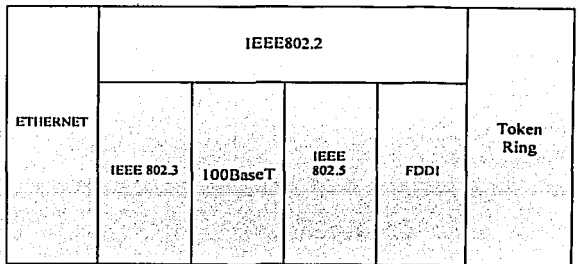
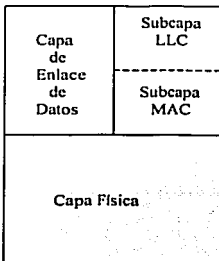




Figura 3.1.1. Esquema de la IEEE.

### 3.2 Logical Link Control (LLC) , IEEE 802.2.

LLC provee los siguientes servicios a la capa de red:

- **Modo sin conexión y sin reconocimiento (Unacknowledged connectionless-mode):** está definido como el Tipo 1 de operación. En este modo las tramas son enviados con la esperanza de que estos llegarán correctamente a su destino; es decir no existe ningún mecanismo de detección de errores y/o retransmisión de información.
- **Modo con conexión (Connection-mode):** está definido como el Tipo 2 de operación. En este modo se establecen, usan, restablecen y terminan conexiones a nivel enlace entre estaciones terminales, permitiendo la retransmisión de tramas en caso de pérdida o transmisión errónea, así como el control de flujo entre estaciones.

El formato del Frame LLC esta formado como se muestra a continuación:

1 Byte DSAP	1Byte SSAP	1 ó 2 Bytes Control	N bytes Información
----------------	---------------	------------------------	------------------------

Donde:

DSAP (Destination Service Address Point):

SSAP(Source Service Address Point):

N

Campo para identificar el proceso de recepción

Campo para identificar el proceso de envío.

Entero mayor o igual a cero.

DSAP/SSAP

El campo DSAP tiene 8 bits, los cuales poseen la siguiente información:

I/G	D	D	D	D	D	D	D
-----	---	---	---	---	---	---	---

Para I/G = 0 la dirección es individual y para I/G=1 se trata de una dirección de grupo.

El campo SSAP tiene 8 bits, los cuales poseen la siguiente información:

C/R	S	S	S	S	S	S	S
-----	---	---	---	---	---	---	---

Para C/R = 0 tenemos un comando en la parte de control, para C/R=1 tenemos una respuesta.

Valores de SAP's más comunes:

04	IBM SNA
06	IP
80	3Com
AA	SNAP
BC	Banyan
E0	Novell
F4	Lan Manager FE -CLNS

TESIS CON  
FALLA DE ORIGEN

Formato del campo de control

Información

1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	
0	N(S)							P/F	N(R)							

Supervisión

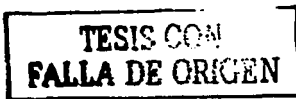
1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16
1	0	S	0	0	0	0	0	P/F	N(R)						

Sin numeración

1	2	3	4	5	6	7	8
1	1	M	0	M			

Donde:

N(S) Número de secuencia de envío  
 N(R) Número de secuencia de recepción  
 S Bits de funciones de supervisión  
 M Bits de funciones no numeradas  
 P/F Bit Poll/Final



### 3.3 MAC (Medium Access Control) o Control de Acceso al Medio

Para la parte MAC, se tiene que existen diferentes técnicas de acceso al medio:

**Por contención:** En esta técnica un dispositivo, para transmitir información, verifica primero que el medio este libre, si lo esta transmite inmediatamente, si no es así, esperará un tiempo finito hasta que el medio de transmisión este libre y de esta manera poder realizar su transmisión. En este tipo de estrategia no existe control de que dispositivo será el siguiente en ocupar el medio de transmisión. Tecnologías típicas que usan este esquema son Ethernet y sus derivadas.

**Round-robin (Rotación circular):** aquí todos los dispositivos que comparten un mismo medio de transmisión tienen asignada una secuencia en tiempos o en turnos para la transmisión de su información de forma rotatoria. Si el dispositivo en turno no tiene nada que transmitir, cede su lugar al siguiente dispositivo en la cola de transmisión. Tecnologías típicas que usan este esquema son Token-Ring y FDDI.

**Por reservación:** se trata del uso de la técnica anterior, pero con la posibilidad de que un dispositivo reserve el siguiente turno de transmisión para si mismo. Tecnologías típicas que usan este esquema son Token-Ring, y FDDI.

El formato del Frame MAC se muestra a continuación y puede diferir un poco, de tecnología en tecnología y esto depende del protocolo MAC en uso, pero en general todas las tramas MAC tienen un formato similar y los campos de esta trama son:

MAC CONTROL	DESTINATION MAC ADDRESS	SOURCE MAC ADDRESS	LLC	FCS
-------------	-------------------------	--------------------	-----	-----

A continuación se muestra la información que contiene cada campo.

MAC CONTROL	Contiene información de control que pudiera ser necesitada para el funcionamiento del protocolo MAC. Por ejemplo, un nivel de prioridad puede ser reservado desde aquí.
DESTINATION MAC ADDRESS	El destino físico para el cuál va dirigido esta trama sobre la red LAN.
SOURCE MAC ADDRESS	El origen físico de la parte que envió esta trama sobre la red LAN.
LLC	LLC indica a quien de la siguiente capa superior va dirigida la información
FCS	Contienen el código generado por un proceso polinomial sobre los campos MAC CONTROL, DESTINATION MAC ADDRESS, SOURCE MAC ADDRESS y LLC. La máquina receptora genera este código cuando recibe la trama y lo compara con el recibido en el mismo. Si son iguales la información esta correcta, si están diferentes, la información tiene errores y la trama es descartada.

El direccionamiento MAC más común para dispositivos de red, usa 6 bytes de acuerdo al siguiente esquema:

3 bytes	3 bytes
Código del fabricante	Número de serie de la interfaz

Generalmente las direcciones MAC se representan con números hexadecimales, separados cada dos números por un punto como por ejemplo 00.B1.FC.00.23.A0.

### 3.4 Ethernet, Fast Ethernet, Gigabit Ethernet

#### 3.4.1 Ethernet

Ethernet es una tecnología LAN muy común dada su simplicidad de operación y de implementación, cuya implementación más frecuente opera a 10 Mbps.

Ethernet fue creado por Xerox en 1972, liberándose la versión 1 de esta tecnología en 1980 por el consorcio DIX (DEC/Intel/Xerox). En 1982 es liberada la versión 2 por el mismo consorcio, iniciándose en el mismo año su estandarización por parte de la IEEE. En 1983 Novell NetWare libera un formato de trama propietario basado en el estándar preliminar de 802.3, 2 años después, la versión final de 802.3 es liberada, la cual incluye el encabezado LLC, haciendo la trama de Netware incompatible. Finalmente el formato 802.3 SNAP fue creado para permitir la compatibilidad entre la Versión 2 de ethernet y 802.3.

##### 3.4.1.1 Topología

En una red de tipo Ethernet, la transmisión hecha por un dispositivo es "escuchada" por todos los demás dispositivos conectados a la misma LAN, la topología lógica empleada es del tipo BUS la cual se implementa físicamente usando cable coaxial como medio de transmisión. Sin embargo, para facilitar su implementación se ha hecho popular el uso del par trenzado como medio de transmisión donde los dispositivos son concentrados a un "hub" o Switch en una topología tipo estrella. Debe enfatizarse que la topología lógica sigue siendo un bus en todos los casos (ver figura 3.4.1.1.1).

TESIS CON  
FALLA DE ORIGEN

## RED LAN ESQUEMA ETHERNET

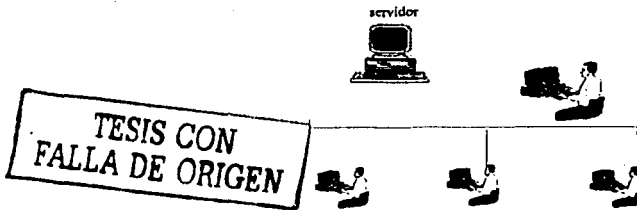


Figura 3.4.1.1.1. Esquema Ethernet

### 3.4.1.2 Implementación física

Dependiendo del medio de transmisión dado y las velocidades de transmisión se tienen las siguientes implementaciones físicas:

Característica	Valores IEEE 802.3				
	10Base5	10Base2	10BaseT	10BaseFL	100BaseT
Tasa de transmisión (Mbps)	10	10	10	10	100
Método de transmisión	Banda Base	Banda Base	Banda Base	Banda Base	Banda Base
Máxima longitud de cable (m)	500	185	100	2,000	100
Medio	50-ohm cable coaxial (thick)	50-ohm cable coaxial (thin)	Par trenzado no apantallado	Fibra óptica	Par trenzado no apantallado
Topología física	Bus	Bus	Estrella	Enlace Repetidor	Bus

En 802.3 las implementaciones físicas son nombradas de acuerdo a ciertas convenciones, las cuales se describen en la siguiente figura:

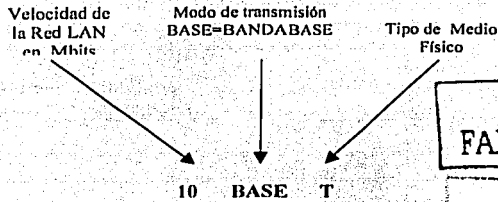


Figura 3.4.1.2.1 Nombres que dependen del tipo de implementación.

### 3.4.1.3 Técnica de acceso al medio (CSMA/CD)

La técnica de acceso al medio que usa Ethernet en cualquiera de sus implementaciones es la llamada CSMA/CD (Carrier Sense Multiple Access with Collision Detection), la cual tiene sus orígenes en la técnica ALOHA, clasificada como de contención. La técnica se desglosa a continuación:

Si un dispositivo tiene información que transmitir:

1. Censa el medio para que nadie este transmitiendo, es decir verifica que el medio de transmisión este libre para su uso. En este momento no existe señal alguna sobre el medio de transmisión.
2. Transmite su información
3. Si el medio esta ocupado, esperará hasta que éste este libre.
4. Si ocurre que dos dispositivos comienzan a transmitir al mismo tiempo, se produce una colisión, la cual es detectada por los dispositivos como una variación inusual de voltaje. Detectada la colisión, se interrumpe inmediatamente la transmisión de la trama, y se transmiten una señal "jam" (32 bits, comúnmente sólo se envían unos) y se espera un tiempo aleatorio para volver intentar acceder al medio.

Es importante recalcar que existen dos tipos de colisiones. La colisión temprana es la que ocurre normalmente en una red ethernet bien dimensionada y consiste en cualquier colisión que ocurre antes de haber transmitido 512 bits en el medio, lo cual permite que los dispositivos involucrados en la colisión detecten la misma y puedan retransmitir la información en proceso de transmisión. Una colisión tardía, consiste en cualquier colisión que ocurre después de haberse transmitido 512 bits en el medio, lo cual no permite que todos los dispositivos involucrados en una colisión se enteren que su información recién transmitida fue dañada y por lo tanto se requiere su retransmisión. Las siguientes figuras ejemplifican la diferencia entre una colisión temprana y una colisión tardía. (ver figuras 3.4.1.3.1 y 3.4.1.3.2 ).

**Secuencia de una colisión temprana:**

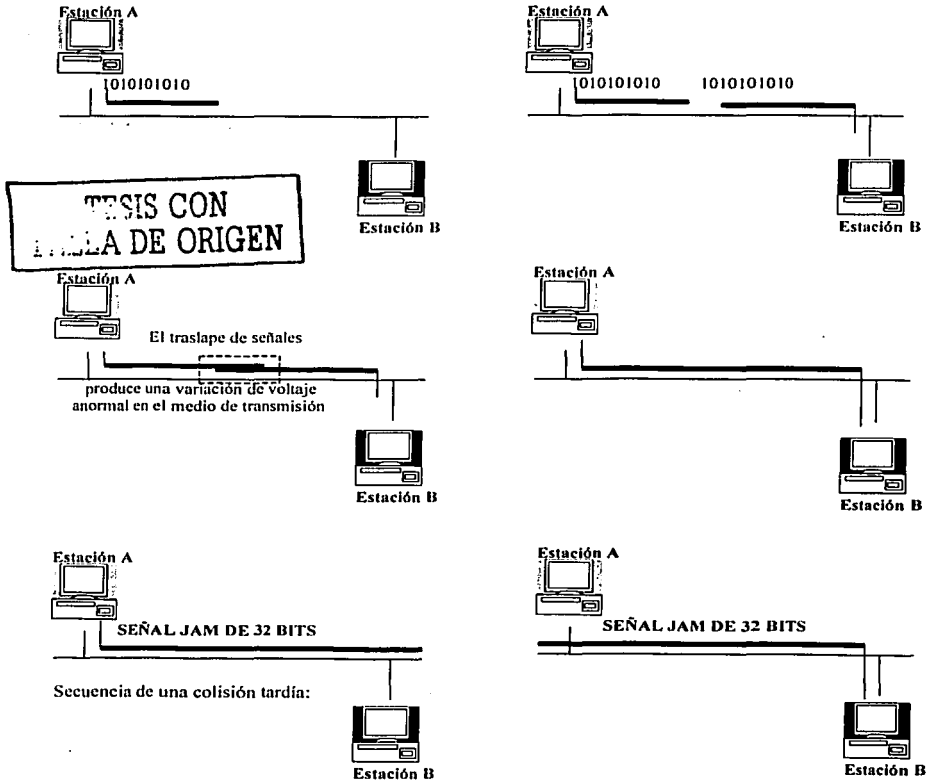


Figura 3.4.1.3.1. Secuencia de una Colisión Temprana

**Secuencia de una colisión tardía:**

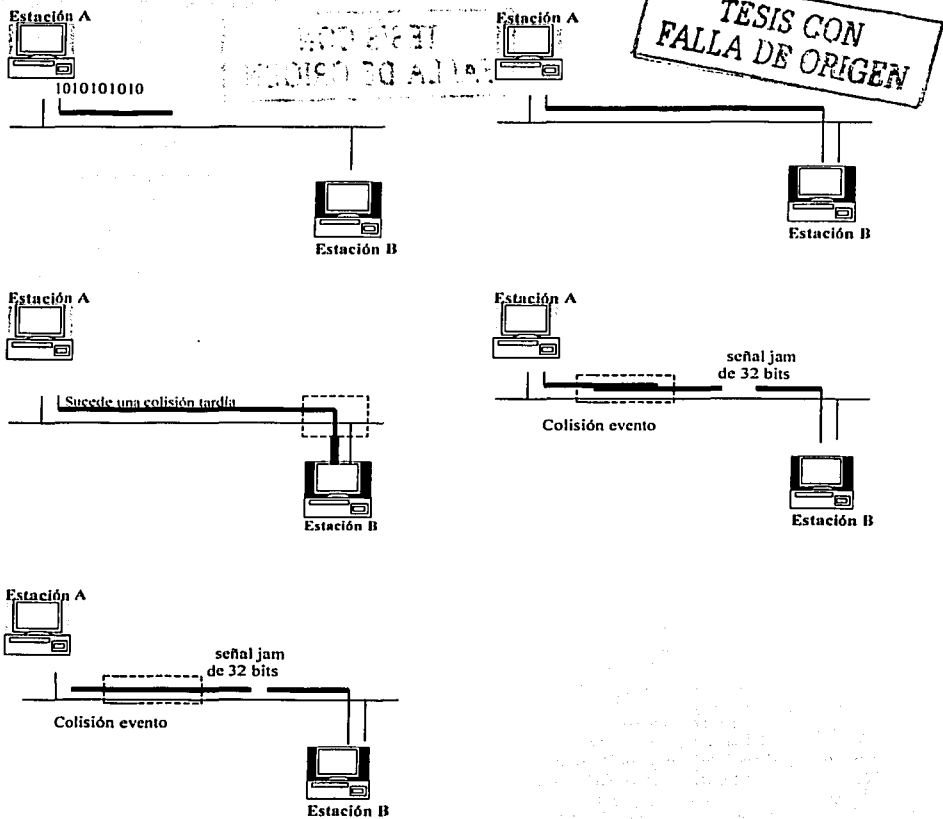


Figura 3.4.1.3.2 Secuencia de Colisión tardía

**3.4.1.4 Formato de Trama.**

Como ya se había mencionado, existen 4 tipos de frame para ethernet, siendo estos Ethernet versión 2, 802.3, Novell y SNAP. Todos ellos tienen una longitud mínima de 64 bytes y una máxima de 1518 bytes (sin contar el campo preamblo).

**TESIS CON  
FALLA DE ORIGEN**

**3.4.1.4.1 Trama ethernet versión 2.**

Esta trama esta formado de los siguientes campos:

- Preamble** Secuencia de 64 bits consistentes en unos y ceros alternados con terminación en "11".  
La sincronía y el inicio del campo de dirección destino (MAC) se logran con este campo.
- DA** Consiste en 6 bytes que contienen la dirección MAC destino.
- SA** Consiste en 6 bytes que contienen la dirección MAC origen.
- Type** 2 bytes que identifican a que protocolo de la capa superior va dirigida la información.
- Data** De 46 a 1500 bytes. Contiene la información destinada a capas superiores.
- FCS** 4 bytes que contienen el código generado por un proceso polinomial sobre los campos DA, SA, Type y Data. La máquina receptora genera este código cuando recibe la trama y lo compara con el recibido en el mismo. Si son iguales la información esta correcta, si están diferentes, la información tiene errores y la trama es descartado.

64 bits	6 bytes	6 bytes	2 bytes	46 a 1500 bytes	4 bytes
Preamble	Destination Address	Source Address	Ether Type	DATA	FCS

**FORMATO DEL FRAME ETHERNET VERSION 2.0**

**3.4.1.4.2 IEEE 802.3.**

Este frame esta formado por los siguientes campos:

- Preamble** Secuencia de 64 bits consistentes en unos y ceros alternados con terminación en "11".  
La sincronía y el inicio del campo de dirección destino (MAC) se logran con este campo.
- DA** Consiste en 6 bytes que contienen la dirección MAC destino
- SA** Consiste en 6 bytes que contienen la dirección MAC origen.
- Lenght** 2 bytes que proporcionan la longitud del campo Data.
- LLC header** 3 bytes de Header LLC o 802.2
- Data** De 43 a 1497 bytes. Contiene la información destinada a capas superiores
- FCS** 4 bytes que contienen el código generado por un proceso polinomial sobre los campos DA, SA, Type y Data. La máquina receptora genera este código cuando recibe la trama y lo compara con el recibido en el mismo. Si son iguales la información esta correcta,



si están diferentes, la información tiene errores y la trama es descartado.

64 bits	6 bytes	6 bytes	2 bytes	1 byte	1 byte	1 byte	43 a 1497 bytes	4 bytes
Preamble	Destination Address	Source Address	Lenght	DSAP	SSAP	Control	DATA	FC

### FORMATO DEL FRAME ETHERNET IEEE 802.3

#### 3.4.1.4.3 Novell (raw).

Este frame consiste de los siguientes campos:

Preamble	Secuencia de 64 bits consistentes en unos y ceros alternados con terminación en "11". La sincronía y el inicio del campo de dirección destino (MAC) se logran con este Campo.
DA	Consiste en 6 bytes que contienen la dirección MAC destino.
SA	Consiste en 6 bytes que contienen la dirección MAC origen.
Lenght	2 bytes que proporcionan la longitud del campo Data.
IPX header	2 bytes nunca usados y puestos en FFFF.
Data	De 44 a 1498 bytes. Contiene la información destinada a capas superiores.
FCS	4 bytes que contienen el código generado por un proceso polinomial sobre los campos DA, SA, Type y Data. La máquina receptora genera este código cuando recibe la trama y lo compara con el recibido en el mismo. Si son iguales la información esta correcta, si están diferentes, la información tiene errores y la trama es descartado.

TESIS CON FALLA DE ORIGEN

64 bits	6 bytes	6 bytes	2 bytes	44 a 1498 bytes	4 bytes
Preamble	Destination Address	Source Address	Lenght	FFFF seguido por los datos	FCS

### FORMATO DEL FRAME NOVELL

#### 3.4.1.4.4 SNAP.

Este frame consiste de los siguientes campos:

Preamble	Secuencia de 64 bits consistentes en unos y ceros alternados con terminación en "11". La sincronía y el inicio del campo de dirección destino (MAC) se logran con este campo
DA	Consiste en 6 bytes que contienen la dirección MAC destino.
SA	Consiste en 6 bytes que contienen la dirección MAC origen.
Lenght	2 bytes que proporcionan la longitud del campo Data.
LLC header	3 bytes de Header LLC o 802.2. DSAP y SSAP están puestos cada uno en AA hexadecimal, el byte de Control identifica el tipo de frame LLC y usualmente tiene el valor de 05 hexadecimal.
Snaf header	Vendor Code: 3 bytes de código de operador, usualmente iguales a los primeros 3 bytes del DA, en otro caso son puestos en cero. Local Code: 2 bytes que contienen usualmente la misma información que el campo Type en Ethernet versión 2.
Data	De 38 a 1492 bytes. Contiene la información destinada a capas superiores.
FCS	4 bytes que contienen el código generado por un proceso polinomial sobre los campos DA, SA, Type y Data. La máquina receptora genera este código cuando recibe la trama y lo compara con el recibido en el mismo. Si son iguales la información esta correcta, si están diferentes, la

información tiene errores y la trama es descartado.

64 bits      6 bytes      6 bytes      2 bytes      1 byte      1 byte      1 byte      5 bytes      38-1492 bytes  
4 bytes

Preamble	Destination Address	Source Address	Lenght	DSAP	SSAP	Control	SNAP	DATA	FC
----------	---------------------	----------------	--------	------	------	---------	------	------	----

### FORMATO DEL FRAME ETHERNET SNAP

#### 3.4.2 Fast Ethernet

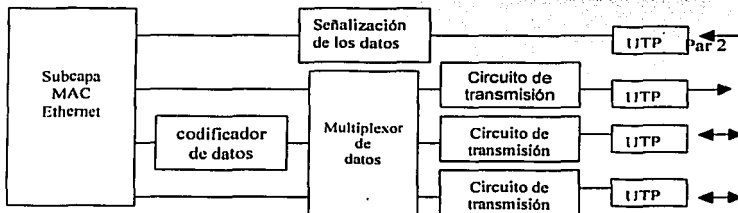
Resultado de la necesidad de una mayor tasa de transmisión, surge Fast Ethernet que opera a 100 Mbps con el mismo formato de frame y técnica de acceso al medio que usa Ethernet a 10 Mbps. Claro, además de la tasa de transmisión tiene algunas diferencias como la auto negociación y el uso opcional de fibra óptica como medio de transmisión.

##### 3.4.2.1 Implementación Física.

La recomendación 802.3u define tres tipos de implementación física para Fast Ethernet:

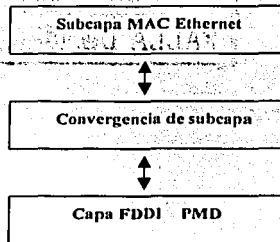
**100baseTX:** Usando UTP categoría 5, se usan dos pares trenzados para la transmisión y recepción de datos.

**100baseT4:** Usando UTP categoría 3, se usan tres pares para la transmisión de datos, y uno para la señalización de los mismos.



**100baseFX:** Implementación sobre fibra multimodo, se utilizan dos fibras, una de transmisión y otra de recepción alcanzándose distancias de 400 metros en transmisión simple duplex y 2 kms en transmisión full duplex.

TESIS CON  
FALLA DE ORIGEN



TESIS CON  
FALLA DE ORIGEN

### 3.4.2.2 Autonegociación.

La Auto-negociación es una característica opcional que habilita el intercambio de información entre dos dispositivos de acuerdo a sus recursos, ya sea a 10 Mbps o a 100 Mbps. La autonegociación es ejecutada mediante el paso de información encapsulada en un tren de pulsos. Estos pulsos son los mismos usados por 10baseT para verificar la integridad del enlace. Si una estación recibe un pulso sencillo, referido como Normal Link Pulse (NLP), este reconoce que el dispositivo en la otra punta sólo es capaz de manejar 10baseT. Si la autonegociación esta siendo usada por una estación, esta transmitirá un tren de pulsos referidos como Fast Link Pulse (FLP). Un FLP consiste de 17 pulsos de reloj interespaciados con 16 pulsos de señal, para formar una palabra código de 16 bits. Si un pulso de señal ocurre entre dos pulsos de reloj, tal bit es 1, si no ocurre pulso de señal, tal bit es cero. La palabra código de 16 bits describe que implementación de ethernet es soportada, de tal forma que las estaciones en autonegociación (regularmente una estación final y un hub o un switch) seleccionen que implementación se usará de acuerdo a las siguientes prioridades:

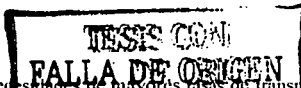
Características	100BaseTX	100BaseEX	100BaseT4
Cable	UTP categoría 5, o STP Tipo 1 y 2	Fibra multimodo 62.5/125 $\mu$ m	UTP categoría 3, 4, o 5
Número de pares o hilos	2 pares	2 hilos	4 pares
Conector	Conector ISO 8877 (RJ-45)	Conector Duplex SCmedia-interface (MIC) ST	Conector ISO 8877 (RJ-45) c
Máxima longitud del segmento	100 metros	400 metros	100 metros
Máxima longitud de la red	200 metros	400 metros	200 metros

100BASE-TX full duplex  
 100BASE-T4  
 100BASE-TX  
 10BASE-T full duplex  
 10BASE-T

La palabra código de 16 bits consta de los siguientes campos:

Selector field (5bits)  
 Technology availability field (8 bits)

Remote fault bit  
Acknowledge bit  
Next page bit



### 3.4.3 Gigabit Ethernet.

Recién surge Fast Ethernet, cuando las necesidades de mayores tasas de transmisión ya están en la puerta, y se desarrolla Gigabit Ethernet. La tasa de transmisión para esta tecnología es de 1 Gbps y se usa básicamente como "backbone" en redes LAN; Gigabit ethernet esta definido en el estándar de la IEEE 802.3z funciona esencialmente de la misma manera que fast ethernet, con la notable diferencia de que opera 10 veces más rápido.

#### 3.4.3.1 Implementación Física.

	1000BASESX	1000BASELX	1000BASECX	1000BASET
TIPO DE CABLEADO	longitud de onda: 850nm fibra multimodo	longitud de onda: 1,300nm fibra multimodo y fibra mono modo	Twin-axial(Twinax)	UTP
RANGO DE DISTANCIAS (metros)	220-550 dependiendo del cable o fibra	550 para fibra multimodo y 5,000 para fibra monomodo	25	100 entre un hub y una estación; un diámetro total de red de 200 m

**1000BaseSX:** también conocido como short-wavelength (por eso el inicio del nombre del medio con S), es apropiado para un cableado de fibra multimodo y para ser el backbone de la red.

**1000BaseLX:** también conocido como longer-wavelength (por eso el inicio del nombre del medio con L), soporta cableado de fibra multimodo y monomodo. 1000BaseLX es apropiado para el soporte de campo del backbone de la red.

**1000BaseCX:** es apropiado para el closet de telecomunicaciones o una sala de computadoras, donde la distancia máxima entre estaciones es de 2.5m o menor. 1000BaseCX puede correr sobre cable de 150-Ohms balanceado, apantallado, cable twinax.

**1000BaseT:** usando cable UTP categoría 5, y puede cubrir una distancia de cableado superior a los 100m, o un diámetro de red de 200m y solo se permite un repetidor.

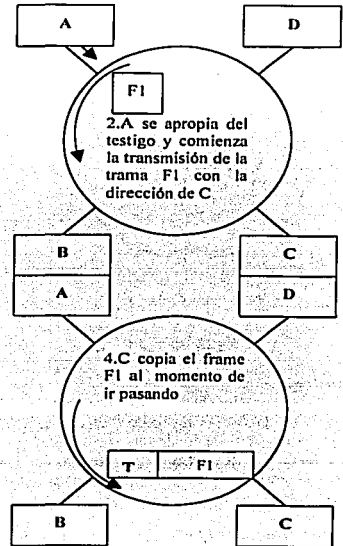
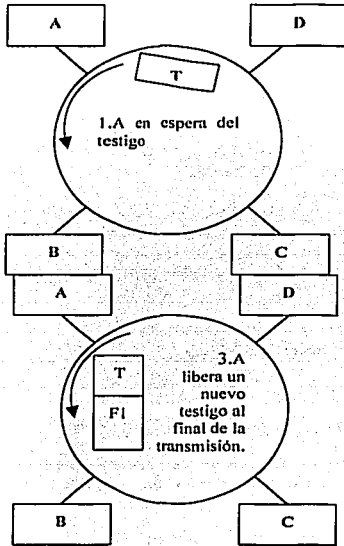
### 3.5 FDDI.

#### 3.5.1 FDDI o interfaz de datos distribuidos por fibra (Fiber Distributed Data Interface).

Proporciona interconexión a alta velocidad entre redes de área local (LAN), y redes de área ancha (WAN). Las principales aplicaciones han entrado en la interconexión de redes LAN Ethernet y de éstas a su vez con redes WAN X.25. Tanto en la conexión de estas tecnologías de red como con otras, todas se conectan directamente a la red principal FDDI (backbone). Otra aplicación es la interconexión de periféricos remotos de alta velocidad a equipos tipo mainframe.

El método de acceso es similar a la de la IEEE 802.5 (Token Ring), con la diferencia que las estaciones negocian el tiempo de circulación y el tiempo de retención del testigo al concertarse con el resto de las

estaciones de la red. El primero es el tiempo máximo que puede tardar el testigo en completar una vuelta al anillo y el segundo es el tiempo máximo que una estación puede retener el testigo para transmitir sus datos. Esto permite tener un retardo de red garantizado, posibilitando, en principio, el tránsito de datos sincrónico, característica que hace factible el envío de voz y vídeo. Lamentablemente FDDI, no puede garantizar el acceso al medio a intervalos de tiempo constantes (el testigo puede estar en poder de otra estación) razón por la cual no permite la transmisión de datos isócronos, como telefonía digital. FDDI utiliza un protocolo de entrega de testigos múltiples. El testigo circula por la red detrás del último paquete transmitido desde un dispositivo. Si una estación desea enviar datos captura el testigo, lo extraerá colocara su paquete o paquetes en el anillo y volverá a colocar el testigo justo a continuación de la corriente de datos. Esto provoca que haya un gran número de tramas circulando por el anillo, cabe aclarar que cada estación es responsable de la absorción de sus propias tramas para que sean retirados del anillo. A continuación con las siguientes figuras se muestra un ejemplo:



TESIS CON FALLA DE ORIGEN

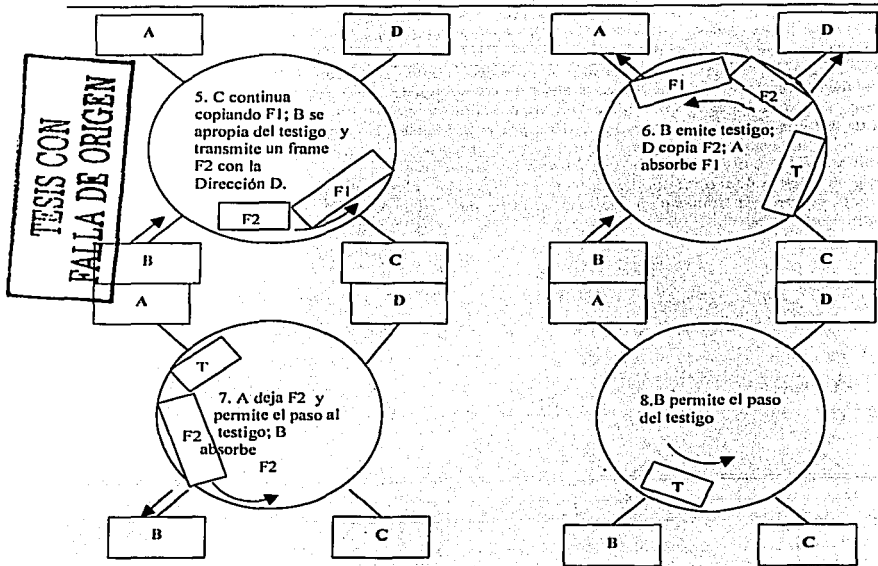


Figura 3.5.1.1 Ejemplo de la circulación y liberación del testigo.

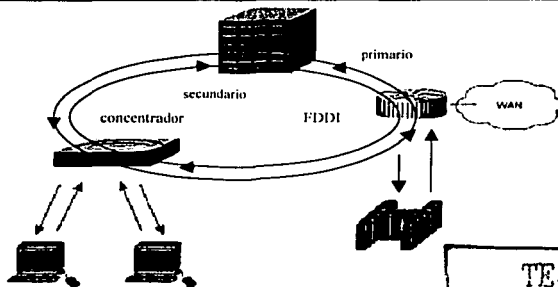
### 3.5.2 Topología.

La topología de la red es de anillo, el cableado de la FDDI está constituido por dos anillos de fibras, uno transmitiendo en el sentido de las agujas del reloj y el otro en sentido contrario, uno principal y otro de respaldo o back-up. El hecho de poseer dos anillos hace que la red FDDI sea altamente tolerante a fallas. El control de la red es distribuido, razón por la cual si falla un nodo real el resto recompone la red automáticamente.

Existen concentradores FDDI que convierten la topología de anillo en estrella, lo cual es más conveniente para cablear.

En una red FDDI puede transmitir a una velocidad de 100 Mbps, pueden coexistir un máximo de 500 estaciones, distanciadas en un máximo de 2 Km. y conectadas por medio de fibra óptica 62,5/125  $\mu\text{m}$  multimodo, en una circunferencia máxima de 100 Km. El error máximo es de  $10^{-9}$  bits.

La norma permite el uso de fibra monomodo y multimodo. La distancia máxima entre las estaciones depende del tipo de fibra que sea utilizada, siendo de 2,5 km. para fibra multimodo (el peor caso). Las estaciones de fibras multimodos son más baratas que las monomodo, pues estas últimas deben utilizar LASER en los transmisores y las primeras simplemente LED (ver la siguiente figura).



TESIS CON FALLA DE ORIGEN

Figura 3.5.2.1. Conexión FDDI

Se define como estación a cualquier equipo concentrador, bridge, router, Hub, estación de trabajo u otro dispositivo conectado a la red FDDI. Los tipos de estaciones que componen una red FDDI son:

**DAS (Dual Attachment Station):** Estación que se conecta tanto al anillo primario como al anillo secundario.  
**DAC (Dual Attachment Concentrator):** Concentrador que permite la conexión de dispositivos de tipo SAS al anillo FDDI.

**SAS (Single Attachment Station):** Estación que se conecta sólo al anillo primario a través de un DAC.

Las estaciones FDDI de clase A (DAS o DAC), usan ambos anillos, ya que tienen la capacidad de reconfigurarse en caso de interrupción del servicio en el primer anillo.

Por el contrario, las estaciones de clase B (SAS y SAC), sólo pueden enlazarse al anillo primario, como solución de conexión de bajo costo, en caso de equipos en donde no es crítica la interrupción del servicio.

La siguiente figura muestra los tipos de elementos que forman una red FDDI.

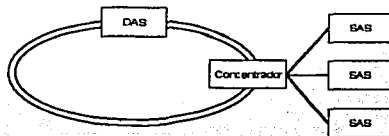


Figura 3.5.2.2. Elementos que conforman a una red FDDI

### 3.5.3 Tolerancia a fallas.

Para garantizar el funcionamiento, cuando una estación está desconectada, averiada o apagada, FDDI implementa varios mecanismos para mantener en operación el anillo.

#### 3.5.3.1 WRAP.

En la figura siguiente la estación 3 falla. Las estaciones 4 y 2 hacen un "wrap" sobre el anillo, es decir, interconectan el anillo primario con el secundario, de tal forma que las estaciones restantes formen un nuevo anillo y mantengan la comunicación.

TESIS CON  
FALLA DE ORIGEN

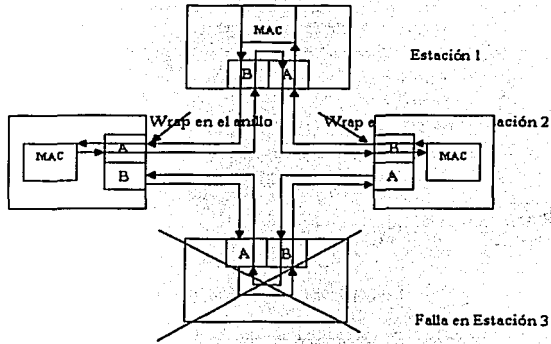


Figura 3.5.3.1.1. WRAP

Cuando la falla ocurre en un enlace (por ruptura de alguna de las fibras), las estaciones vecinas hacen también un "wrap" de los anillos primario y secundario, de tal forma que se mantenga la comunicación en todas las estaciones. Esto está representado en la siguiente figura.

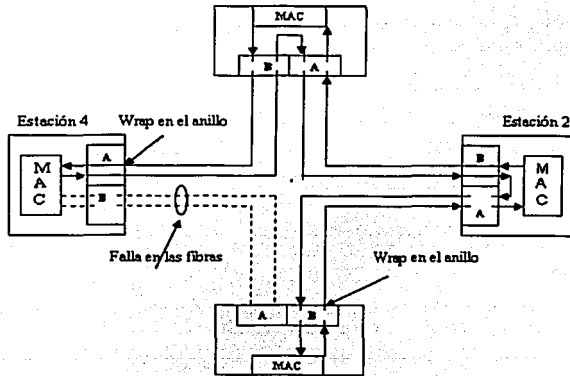
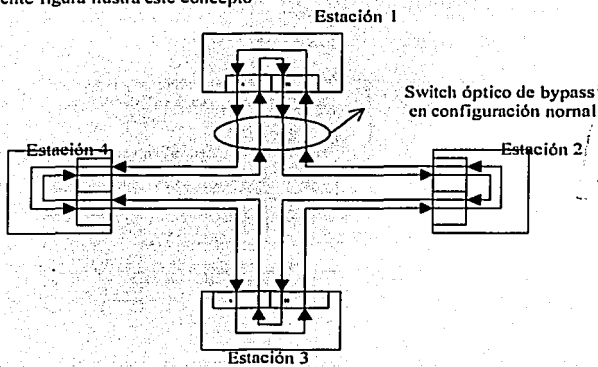


Figura 3.5.3.1.2 Falla por ruptura de fibras



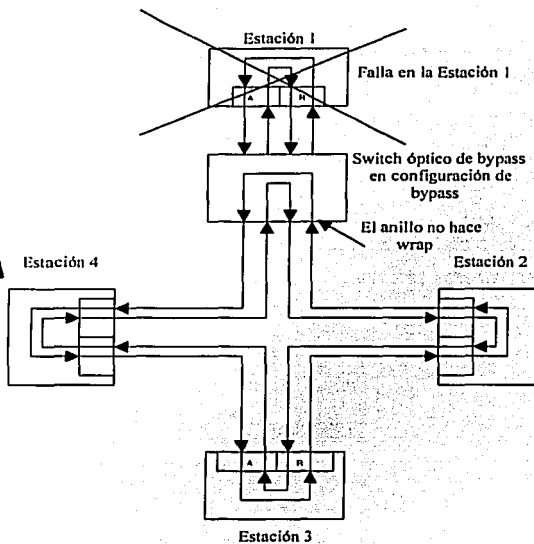
### 3.5.3.2 Bypass.

Se encarga de mantener en operación los anillos primario y secundario, sin hacer "wrap" cuando una estación ha fallado. La siguiente figura ilustra este concepto



TESIS CON FALLA DE ORIGEN

TESIS CON  
FALLA DE ORIGEN



Estación 3  
Figura 3.5.3.2.1 Configuración de bypass

### 3.5.3.3 Dual Homing.

Dispositivos críticos, tales como Main tramas, enrutadores y otros equipos, pueden usar la técnica llamada Dual Homing para proveerles redundancia adicional. En escenarios de este tipo, el dispositivo o estación crítica es conectado a dos concentradores. Uno de los enlaces es declarado como activo y proveerá la comunicación del dispositivo. El enlace restante es declarado como pasivo, y estará como respaldo hasta que el enlace primario falle, activándose de forma automática. La siguiente figura ilustra un escenario Dual Homing.

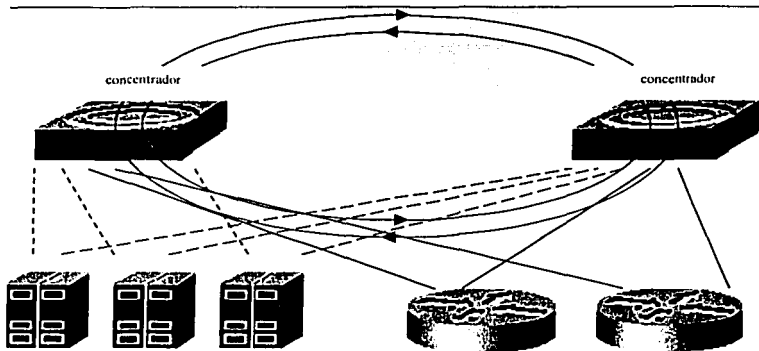


Figura 3.5.3.2.1 Técnica Dual Homing

### 3.5.4 Arquitectura.

En la estructura FDDI, se distinguen 4 subcapas básicas, cada una con funciones totalmente separadas:

#### 3.5.4.1 PMD o Physical Media Dependent (dependencia del medio físico).

Especifica las señales ópticas y formas de onda a circular por el cableado, incluyendo las especificaciones del mismo así como las de los conectores.

Dentro del modelo OSI, la capa física ocupa el menor nivel, esta se encarga de definir la transmisión de bits en el medio físico.

La norma PMD especifica:

- Características y tipos de transmisores, receptores, cables, conectores, etc. Tomando en cuenta funcionalidad y economía.
- Establece como nodos físicos a los conectados al anillo FDDI y como estaciones a las interconectadas físicamente a la red por un medio de cobre o fibra óptica.

Define varias opciones:

Fibra Multimodo (MMF-PMD)  
 Fibra Monomodo (SMF-PMD)  
 Fibra de Bajo Costo (LCF-PMD)  
 Par Trenzado Apantallado (STP-PMD)  
 Par Trenzado Sin Apantallar (UTP-PMD)  
 FDDI Sobre SONET (Synchronous Optical Network)

TESIS CON  
 FALLA DE ORIGEN

---

MMF-PMD.- 62.5/125  $\mu\text{m}$  de índice graduado), la emisión de luz es utilizando diodos emisores de luz (LED's transmisores de 1300 nanómetros (nm)), con lo que se consigue una transmisión óptima en enlaces de hasta 2 Km. Este es el primer estudio realizado por la ANSI.

SMF-PMD.- La fuente de luz requerida es una fuente láser, lo que provee un mayor poder que la fuente led. Existen dos categorías de dispositivos para transmisión y recepción de luz, los cuales se separan en Categoría I y II. Los de categoría

I cumplen con las especificaciones de la norma MMF mientras que la Categoría II utiliza dispositivos con mayor poder y sensibilidad que los de la categoría I. Con categoría II se puede llegar a distancias de 60 Km. (con una atenuación de 0,5 db/Km)

LCF.- Utiliza componentes de bajo costo como transmisores y receptores, Otra característica es el uso de fibra monomodo de 62,5/125  $\mu\text{m}$  de índice graduado. Los tramos utilizados de fibra entre estaciones pueden llegar a cubrir una distancia máxima de 500 metros. Es una solución de bajo costo para el PMD, con el cual pueden mezclarse los distintos PMD para obtener una red completa, por ejemplo, puede usarse SMF para el anillo principal y LCF para las uniones departamentales.

### 3.5.4.1.2 Funciones del PMD

Dentro de las funciones del PMD, se tiene que para ser transmitidos los datos entre estaciones, estos son reunidos primeramente en bits de datos en una serie de señales y luego se transmiten estas señales sobre el cable de unión entre las dos estaciones. La norma PMD trata con todas las áreas que son asociadas con la transmisión física de los datos, como son:

- Transmisores y receptores ópticos y eléctricos
- Fibra óptica o cable de cobre
- Interfaz de conexión al medio (MIC), Conectores
- Retardo por desvío óptico

La norma PMD asegura que los transmisores, cableados y receptores interactúan cuando se le especifican los parámetros que son propiamente implementados:

- Proporciona a la capa física los servicios requeridos para transportar un flujo de bits codificados al nodo siguiente.
- Proporciona a la capa PHY los datos recibidos del medio físico en forma de señales NRZI, Codificados eléctricamente.
- Proporciona a la capa SMT los servicios requeridos para un manejo apropiado del anillo.
- Las capas PMD y PHY intercambian datos a una velocidad de 125 Mbps
- Las medidas de fibra multimodo más utilizadas son: 62,25/125, 50/125 100/140 micrones.
- La fibra multimodo "STEP Index" no reúne los requisitos de ancho de banda para FDDI por lo tanto no esta permitida.
- La norma FDDI PMD especifica la potencia supuesta de 11.0db y una atenuación máxima del cable de 1.5 dB/Km. Para una longitud de onda de 1300nm.
- Ventanas y Operación de Longitud de Onda

### 3.5.4.1.3 Conector Medio-Interface

El Modelo ANSI define los medios para conectar físicamente un cable a una estación FDDI, como:

Conectores MIC

Los conectores MIC se usan habitualmente para conectar fibra óptica a una estación FDDI.

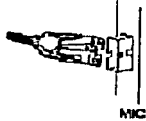


Figura 3.5.4.1.3.1 Conectores MIC para fibra óptica a una estación FDDI

#### 3.5.4.1.4 Tipos de puertos.

Especifican reglas de conexión para asegurar el funcionamiento ante la construcción de topologías ilegales. En las topologías FDDI hay 4 tipos de puertos: A, B, M, y S.

##### Tipos de Puertos

**Puerto A.-** Conecta al anillo primario que entra y el anillo secundario de salida del anillo FDDI. Este puerto es parte de una estación de conexión Doble ("DAS") o un Concentrador Dual ("DAC").

**Puerto B.-** Conecta al anillo primario de salida y al anillo secundario de entrada del doble anillo FDDI. Este puerto es parte de un DAS o un DAC y también se usa para conectar un DAS a un concentrador.

**Puerto M.-** Conecta un concentrador a una estación de conexión simple (SAS), DAS u otro Concentrador de conexión simple (SAC). Este puerto se implementa sólo en un concentrador (DAC, SAC)

**Puerto S.-** Conecta un SAS o un SAC a un concentrador (DAC o SAC).

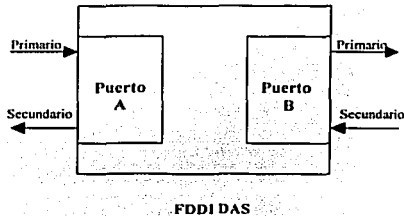
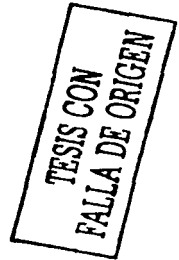


Figura 3.5.4.1.4.1 Tipos de puertos



#### 3.5.4.1.5 Derivador óptico (Relay Bypass Óptico)

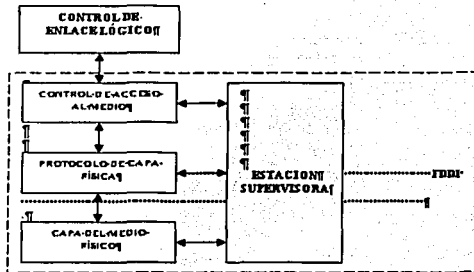
La opción de bypass puede ser utilizado para mantener la conectividad del anillo FDDI. El Bypass permite relevar la luz al receptor óptico en una estación defectuosa. De este modo la estación defectuosa es aislada y se mantiene la operación del anillo FDDI.

Los Bypass no efectúan funciones de repetidores, de amplificadores ni restablecimiento de flujo de bit.

Para una estación aislada, la nueva distancia entre estaciones adyacentes puede exceder el máximo valor permitido.

Los Bypass, como aparato mecánico, puede fallar, luego la integridad del anillo doble dependen de la integridad de este.

¡ATENCIÓN!  
SISTEMA DE ALTA VELOCIDAD



### 3.5.4.2 PHY o Physical Layer Protocol (protocolo de la capa física).

Se encarga de la codificación y decodificación de las señales así como de la sincronización, mediante el esquema 4-bytes/5-bytes, que proporciona una eficacia del 80%, a una velocidad de señalización de 125 MHz, con paquetes de un máximo de 4.500 bytes. Proporciona la sincronización distribuida. Fue aprobada por ANSI en 1988 y se corresponde con la mitad superior de la capa 1 en el esquema OSI.

La norma de la capa PHY, define aquellas partes de la capa física que son independientes del medio.

El Protocolo de la capa física define lo siguiente:

- Recuperación de reloj y datos: Recupera la señal de reloj desde los datos ingresados.
- Proceso de Codificación/Decodificación: Convierte los datos desde la MAC al interior de una transmisión sobre el anillo FDDI.
- Símbolos: Son las más pequeñas señales existentes usadas para comunicación entre estaciones. Los símbolos están comprimidos en códigos de 5 bits.
- Elasticidad Topé: Estimación de las tolerancias para reloj entre estaciones.
- Función de Alisamiento: Corrige tramas que han perdido el encabezamiento.
- Filtro repetidor: Corrige la violación del código e invalida estados de la línea.
- Recuperación de Reloj y Datos

La norma FDDI PHY especifica el uso del reloj distribuido sobre la red. Cada Estación tiene un reloj generado localmente para la transmisión o repetición de información sobre el anillo.

La estación Receptora sincroniza su reloj receptor al flujo de símbolos de entrada. La estación decodifica los datos usando este reloj. Cuando transmite el dato, usa el reloj local como reloj fuente.

#### 3.5.4.2.1 Proceso de Codificación.

La Unidad básica de Información usada en la codificación de FDDI es el "Símbolo". Los símbolos se usan para transmitir información entre estaciones de la red FDDI. Para transmitir tramas, el PHY convierte la información recibida desde la MAC en un flujo de bits codificados.

Para realizar la codificación, FDDI utiliza tanto el codificador 4B/5B como el NRZ/NRZI. Una vez que el símbolo pasa a través del codificador 4B/5B, pasa a través del codificador NRZ/NRZI.

---

El Codificador 4B/5B, usando el esquema anterior el PHY convierte los símbolos de 4 bits en código de 5 bits para transmisión sobre el medio. El uso de grupo de código de 5 bits se basa en que el FDDI tenga una:

- Velocidad de señalización de 125 megabaudios.
- Velocidad de datos de 100 Mbps.

#### 3.5.4.2.2 Símbolos.

FDDI Define tres tipos de símbolos:

- Símbolos de datos. Representa el dato actual que está siendo enviado.
- Símbolos de estado de línea: Usado para la comunicación entre PHYs adyacentes.
- Símbolos indicadores de control: Muestran el estado de la trama
- Símbolo de dato.

De los 32 símbolos usados en FDDI, solo 16 de estos representan datos. El dato está representado en forma hexadecimal. El resto de los símbolos definen el estado de línea y condiciones de control.

##### 3.5.4.2.2.1 Símbolo de estado de línea.

Los estados de línea son secuencias de símbolos que se usan para la señalización PHY. Grupos de símbolos de estados de línea se usan para comunicar PHYs adyacentes. Esta comunicación se usa cuando inicia la conexión.

##### 3.5.4.2.2.2 Símbolos Indicadores de Control.

Estos símbolos se usan para indicar el estado de una trama que se desplaza alrededor del anillo. Alguno de los estados de información transportados por los símbolos de control incluyen lo siguiente:

**Error Detectado:** Colocado por una estación que detecta un error.

**Reconocimiento de dirección:** Colocado por una estación que reconoce una trama dirigida a ella.

**Copiado de trama:** Colocado por una estación que copia la trama.

**Elasticidad Topo:** Estimación de las tolerancias para reloj entre estaciones. Cada estación usa un reloj generado localmente para transmitir los datos. Las frecuencias de los datos son estrictamente controladas entre estaciones, por ellas nunca son idénticas.

**Función de Alisamiento:** Corrige tramas que han perdido el encabezamiento.

**Filtro repetidor:** Corrige la violación del código e invalida estados de la línea. Este filtro previene la propagación de violaciones de código e invalida estados de línea. El filtro repetidor permite:

Propagación de tramas válidas, Propagación de tramas dañadas, tales que ellas puedan ser contadas por el próximo MAC existente en el anillo.

El filtro repetidor también incluye mecanismos para minimizar los efectos de fragmentación de tramas, los cuales son tramas parciales a la izquierda del anillo en ciertas operaciones MAC.

#### 3.5.4.2.3 MAC o Media Access Control (control de acceso al medio).

---

Su función es la programación y transferencia de datos hacia y desde el anillo FDDI, así como la estructuración de los paquetes, reconocimiento de direcciones de estaciones, transmisión del testigo, y generación y verificación de secuencias de control de tramas (FCS o Frame Check Sequences). Se corresponde con la mitad inferior de la capa OSI 2 (capa de enlace de datos) y fue aprobada por ANSI en 1986.

#### 3.5.4.2.3.1 Control de Acceso al Medio.

Las normas MAC definen lo siguiente:

- Acceso justo e igual al anillo a través del uso de un protocolo de señales de tiempo.
- Comunicación entre dispositivos unidos usando tramas y señales.
- Construcción de tramas y señales
- Transmisión, Recepción y Desmembramiento (stripping) de tramas y señales desde el anillo.
- Varios mecanismos de determinación de errores.
- Iniciación del anillo.
- Aislación de fallas del anillo (o de anillos fallando, o defectuosos)
- Comunicación sobre el anillo.

Un anillo FDDI consta de estaciones conectadas en serie por medio de tramos que forman un lazo cerrado. El dato es transmitido serialmente como un flujo de símbolos desde una estación a otra. Cada estación en turno regenera y repite cada símbolo, pasando el símbolo a la estación siguiente. Se han diferenciado dos clases de servicios sobre una red FDDI.

#### 3.5.4.2.3.2 Clases de servicio: síncrono y asíncrono.

La clase de servicio síncrono responde a aplicaciones que necesitan una banda de paso de alta capacidad y/o un tiempo de propagación en el enrutamiento determinado, en otras palabras, tráfico síncrono es la voz, imágenes, o cualquier tipo de información que debe ser transmitida antes de un determinado tiempo. Podrá decirse que es tráfico de datos en tiempo real, y es este el tipo de tráfico que tiene prioridad en FDDI.

La clase de servicio asíncrono satisface los inconvenientes de tráfico de tipo síncrono, presentando cierta cantidad de banda de paso compartida por todas las estaciones que utilicen este método. Tráfico de aplicaciones como correo electrónico y ftp son exponentes típicos de este tipo de servicio y en general cualquier información para la cual el tiempo que tarde en llegar al destino no es factor decisivo, FDDI comparte el ancho de banda entre todas las estaciones que transmiten este tipo de tráfico.

#### 3.5.4.2.3.3 Definición de Tramas MAC.

La máxima longitud de la trama FDDI es limitada a 9000 símbolos o 4500 bytes para evitar problemas de desincronización. La longitud máxima de 4,500 bytes es determinada por la codificación empleada, denominada 4B/5B (4 bytes/5 bytes), con una frecuencia de reloj de 125 MHz, siendo por tanto la eficacia del 80%. El formato de la trama es:

PA = Preámbulo 4 o más símbolos de Idle. (Para sincronismo).

SD = Delimitador de Inicio (Utiliza los símbolos "J" y "K")

FC = Control de Trama. Tipo de Trama (Síncrona o Asíncrona)

DA = Dirección Destino (Utiliza 12 símbolos o hasta 6 bytes)

SA = Dirección Fuente (Utiliza 12 símbolos o hasta 6 bytes)

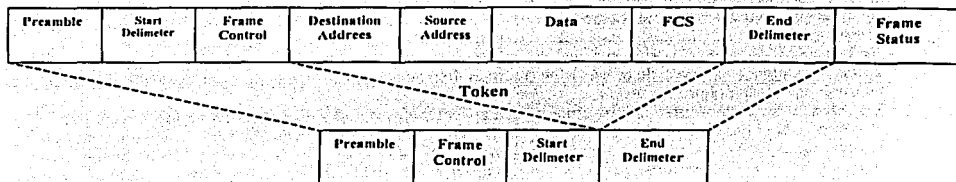
INF= Información ( N Bytes..)

FCS= Redundancia de la trama (con CRC-32)



ED = Delimitador de Fin de Trama. (Utiliza el símbolo "T")  
FS = Estado de la trama. (Trama Errónea, bien recibida... Etc).

#### FRAME DE DATOS



#### 3.5.4.2.4 SMT o Station Management (gestión de estaciones).

Se encarga de la configuración inicial del anillo FDDI, y monitorización y recuperación de errores. Incluye los servicios y funciones basadas en tramas, así como la gestión de conexión (CMT o Connection Management), y la gestión del anillo (RMT o Ring Management). Se solapa con las otras 3 subcapas FDDI, y por tanto fue la de más complicada aprobación por parte de ANSI, que se realizó en 1993.

Provee los servicios necesarios en el nivel de estación, para el monitoreo y control en una estación FDDI. SMT Permite a las estaciones de trabajo cooperadoras al interior del anillo y asegura la operación propia de la estación. Realiza el monitoreo de la red FDDI más fácilmente y permite la operación normal. Usando los servicios proporcionados por las capas PMD, PHY y MAC.

Puede realizar muchas funciones tales como: Inicialización e indicación del nodo, recuperación y aislamiento de fallas, recolección y manejo de ancho de banda entre diferentes clases de prioridades de mensajes.

El SMT posee tres componentes mayores:

- Administración de Conexión (CMT)
- Administración de Anillo (RMT)
- Servicios de trama SMT

#### 3.6 Resumen.

En este capítulo se describieron las tecnologías LAN más importantes, además se enfatizó más en los detalles del funcionamiento, así como la información y campos con los que se conforma la trama de datos respectivo dependiendo la tecnología LAN en uso.

TESIS CON  
FALLA DE ORIGEN

---

## Capítulo 4. Tecnologías WAN.

### 4.1 Definición.

Una red de área amplia o WAN (Wide Area Network), se extiende sobre un área geográfica extensa, que tienen la capacidad de interconectar países o continentes; contiene un número variado de *hosts* dedicados a ejecutar programas de usuario (de aplicación). Los *hosts* están conectados por una subred de comunicación, o simplemente subred. El trabajo de la subred es conducir mensajes de un *host* a otro.

En muchas redes WAN, la subred tiene dos componentes distintos: las líneas de transmisión y los elementos de conmutación. Las líneas de transmisión (también llamadas circuitos o canales) son el medio donde los bits se mueven de una máquina a otra.

Los elementos de conmutación son equipos que conectan dos o más líneas de transmisión. Cuando los datos llegan por una línea de entrada, el elemento de conmutación debe escoger una línea de salida para enviarlos.

En casi todas las WAN, la red contiene numerosos cables o líneas telefónicas, cada una conectada a un par de enrutadores. Si dos enrutadores que no comparten un cable desean comunicarse, deberán hacerlo indirectamente, por medio de otros dos enrutadores. Cuando se envía un paquete de un enrutador a otro a través de uno o más enrutadores intermedios, el paquete se recibe completo en cada enrutador intermedio, se almacena hasta que la línea de salida requerida está libre, y a continuación se reenvía. Una subred basada en este principio se llama, de punto a punto, de almacenar y reenviar, o de paquete conmutado. Casi todas las redes de área amplia (excepto aquellas que usan satélites) tienen subredes de almacenar y reenviar.

Otra posibilidad para una red WAN es un sistema de satélite o de radio en tierra. Cada enrutador tiene una antena por medio de la cual puede enviar y recibir. Todos los enrutadores pueden oír las salidas enviadas desde el satélite y en algunos casos pueden oír también la transmisión ascendente de los otros enrutadores hacia el satélite. Algunas veces los enrutadores están conectados a una subred punto a punto de gran tamaño, y únicamente algunos de ellos tienen una antena de satélite. Por su naturaleza, las redes de satélite son de difusión y son más útiles cuando la propiedad de difusión es importante.

### 4.2 Redes de conmutación de circuitos y conmutación de paquetes.

#### 4.2.1 Redes de Conmutación de Circuitos.

En este tipo de redes se establece un camino dedicado entre las terminales finales, constituido por recursos dedicados en los centros de conmutación y enlaces de transmisión entre los mismos, de forma que se emplea todo el ancho de banda del medio de transmisión para esa conexión, es decir, por el medio de transmisión irán única y exclusivamente las informaciones que se intercambien los terminales.

En la transferencia de información se distinguen tres fases claramente diferenciadas:

- a) **Establecimiento del circuito.** En esta fase se establece el circuito entre los dispositivos implicados en la comunicación. El terminal que inicia la comunicación envía a la red información de señalización indicando que desea conectar con el terminal destino y queda en espera hasta recibir señalización de comunicación establecida. La red asigna recursos de forma exclusiva a la comunicación, tanto en los centros de conmutación como en los medios de transmisión.
- b) **Transferencia de información.** Una vez que está establecida la comunicación, se dispone de un circuito dedicado a través de la red. La red no introduce retardo ni realiza ningún tratamiento de la información. Los terminales de datos han de trabajar a la misma velocidad y emplear protocolos comunes, ya que al ser la red un elemento totalmente pasivo no realiza conversión de velocidades ni de protocolos.
- c) **Liberación de la comunicación.** Bajo la iniciativa de cualquiera de los dos terminales implicados en la comunicación la red libera los recursos asignados a la comunicación.

En fase de transferencia de datos, si hubiera espacios de tiempo sin comunicación, se desperdiciaría la capacidad asignada en la red.

Se puede observar que las redes telefónicas emplean esta técnica en una comunicación normal por teléfono: la fase de establecimiento del circuito consiste en marcar (indicación del deseo de comunicar) y esperar mientras la red crea la conexión, hasta que el destino toma el aparato después de ser avisado con el timbre.

Durante la transferencia de información, cualquiera de los dos interlocutores pueden intercambiar todo tipo de datos (en forma de voz) con el otro. Mientras dura esta comunicación, nadie más puede utilizar las líneas ni los aparatos que están implicados; por ejemplo, nadie podrá llamar a otra persona hasta que una de las partes finaliza la comunicación. Finalmente, se libera la comunicación cuando cualquiera de los dos cuelga el teléfono, indicando a la red que puede dejar libre el medio de transmisión, ya que el enlace creado ha dejado de ser útil.

Las prestaciones que proporcionan los sistemas de conmutación de señales telefónicas no son adecuadas para conmutación de datos, debido sobre todo a los elevados tiempos de establecimiento de las comunicaciones (del orden de varios segundos) y al desperdicio de ancho de canal al tener que ser usado únicamente para una comunicación.

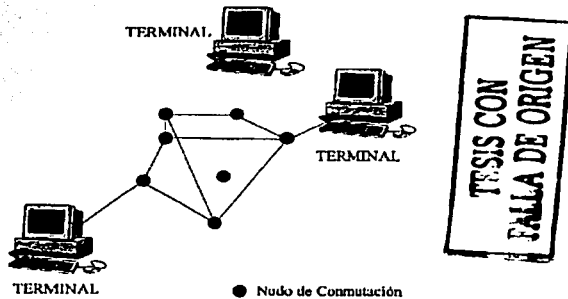


Figura 4.2.1.1 Red de Conmutación de Circuitos

#### 4.2.2 Redes de Conmutación de Paquetes.

La idea de la conmutación de paquetes es aprovechar las características de la conmutación de mensajes en cuanto al compartir de la infraestructura de transmisión y conmutación, multiplexando la información de las diversas comunicaciones y rebajar así el tiempo de tránsito de la información por la red.

Para ello, se limita el tamaño de los mensajes y el almacenamiento en los centros de conmutación se realiza en memorias de acceso directo consiguiendo que se reduzca el tiempo que pasa un paquete de información en la red.

Como en el caso de la conmutación de mensajes, no se reservan recursos con anterioridad, sino que se utilizan siempre que sean necesarios (pero si no hay espacio libre, se pierden).

La información se formatea en bloques de pequeño tamaño denominados paquetes. Un paquete es un grupo de dígitos binarios que incluyen datos e información de control y que es tratada de forma autónoma por la red. Los terminales envían la información partida en paquetes al nodo de la red al que estén conectados.

En cada nodo los paquetes se almacenan en las colas de entrada (memoria de acceso directo) hasta que se procesan (conmutan). La conmutación consiste básicamente en decidir por qué línea de salida se envía el paquete. A continuación, se almacena en las colas de salida (memoria de acceso directo) hasta su transmisión por la línea.

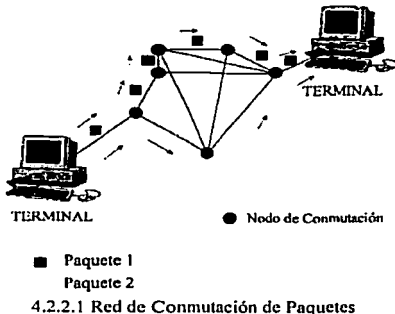
En resumen, la técnica de conmutación de paquetes consiste en la multiplexación asíncrona de paquetes con dirección, tanto en los medios de transmisión como en los centros de conmutación. De esta forma se logra la utilización óptima de la red, porque siempre que haya información en las colas de los nodos, los recursos de comunicaciones de la red se están aprovechando para cursar tráfico.

Estas redes permiten la concentración de comunicaciones por un mismo medio de comunicación. Muchas organizaciones disponen de recursos informáticos centralizados (centros de cálculo, bases de datos, etc.) a los que necesitan acceder desde localizaciones remotas, con terminales. Mediante la conmutación de paquetes el recurso centralizado puede comunicarse simultáneamente con varios terminales por una única línea de comunicación.

En conmutación de circuitos debería emplearse tantas líneas como comunicaciones simultáneas quisieran mantenerse, porque cada enlace establecido reservaría una línea en exclusiva para cada comunicación.

El diseño de las redes de paquetes se optimiza para que el tránsito total de un paquete por la red sea inferior a un segundo, lo que en la práctica permite cursar el tráfico de la mayoría de las aplicaciones interactivas, como vídeos, televisión interactiva, etc.

TESIS CON  
FALLA DE ORIGEN



### 4.3 Capa Física: WAN.

#### 4.3.1 Tipos de interfaces.

La capa física WAN describe la interfaz entre el equipo terminal de datos (DTE) y el equipo de conexión de los datos (DCE). Típicamente, el DCE es el proveedor de servicio, y el DTE es el dispositivo asociado. En este modelo, los servicios ofrecidos al DTE se hacen disponibles a través de un módem o unidad de servicio del canal/unidad de servicios de datos (CSU / DSU).

---

Algunos estándares de la capa física que especifican esta interfaz son:

- EIA/TIA-232D: Esta norma fue definida como una interfaz estándar para conectar un DTE a un DCE.
- EIA/TIA-449: Junto a la 422 y 423 forman la norma para transmisión en serie que extienden las distancias y velocidades de transmisión más allá de la norma 232.
- V.35: Según su definición original, serviría para conectar un DTE a un DCE síncrono de banda ancha (analógico) que operara en el intervalo de 48 a 168 kbps.
- X.21: Estándar CCITT para redes de conmutación de circuitos. Conecta un DTE al DCE de una red de datos pública.
- G.703: Recomendaciones del ITU-T, antiguamente CCITT, relativas a los aspectos generales de una interfaz a velocidades de 2,048 kbps.
- EIA-530: Presenta el mismo conjunto de señales que la EIA-232D.
- High-Speed Serial Interface (HSSI): Estándar de red para las conexiones seriales de alta velocidad (hasta 52 Mbps) sobre conexiones WAN.

#### **4.4 Tipos de conexiones WAN.**

##### **4.4.1 Enlaces dedicados (Conexiones dedicadas).**

Un enlace dedicado punto a punto provee un canal de comunicaciones o camino pre-establecido WAN en el cual se transporta toda la información del cliente. El canal o camino que se destina para la información del cliente es permanente y es de uso exclusivo por lo cual esta reservado en todo momento para el uso privado del mismo. El rango de velocidad va desde un enlace de 64 Kbps (DS-0) hasta 10 Gbps (STS-192). En las empresas se emplea la línea dedicada para el tráfico de voz y datos a la vez. En esta tecnología el tráfico de datos es típicamente encapsulado en un protocolo estándar que puede ser PPP o HDLC.

Como regla general, las conexiones de un enlace dedicado tienen mayor costo- efectividad cuando presentan las siguientes condiciones:

- Tiempo de conexión elevado
- Distancias cortas

##### **4.4.2 Enlaces vía circuitos virtuales.**

Es un método en el cual los medios con los cuales se obtiene el enlace no son privados, como el caso de un enlace dedicado, el enlace también se realiza punto a punto en el cual se transportan paquetes desde un punto origen a un punto destino a través de una infraestructura de red. Este tipo de enlace utiliza la conmutación de paquetes y se realiza a través de circuitos virtuales (VC's) que proveen el end-to end en cuanto a conexión.

##### **4.4.3 Enlaces conmutados.**

Es un método que se utiliza por medio de un circuito físico dedicado que inicia, mantiene y termina con la sesión de comunicación que se establece. En este tipo de enlace se realiza una etapa de señalización en la cual se determinan los puntos y la conexión entre los dos puntos finales.

El método de conmutación de circuitos requiere que se realice una llamada y la terminación de la misma para el inicio y terminación de la conexión respectivamente. Este método es usado en la compañía de redes telefónicas.

#### **4.5 Protocolos WAN usados sobre conexiones WAN dedicadas y conmutadas.**

---

Los protocolos WAN más comunes en la capa de enlace de datos, asociadas con conexiones dedicadas y conmutadas se enumeran a continuación:

- Synchronous Data Link Control (SDLC). Es un protocolo orientado a bit desarrollado por IBM. SDLC define un ambiente WAN multipunto que permite que varias estaciones se conecten a un recurso dedicado. SDLC define una estación primaria y una o más estaciones secundarias. La comunicación siempre es entre la estación primaria y una de sus estaciones secundarias. Las estaciones secundarias no pueden comunicarse entre sí directamente.
- High-Level Data Link Control (HDLC). Es un estándar ISO. HDLC no pudo ser compatible entre diversos vendedores por la forma en que cada vendedor ha elegido cómo implementarla. HDLC soporta tanto configuraciones punto a punto como multipunto.
- Link Access Procedure Balanced (LAPB). Utilizado sobre todo con X.25, puede también ser utilizado como transporte simple de enlace de datos. LAPB incluye capacidades para la detección de pérdida de secuencia o extravío de tramas así como también para intercambio, retransmisión, y reconocimiento de tramas.
- Point-to-Point Protocol (PPP). Descrito por el RFC 1661, dos estándares desarrollados por el IETF. El PPP contiene un campo de protocolo para identificar el protocolo de la capa de red.

#### 4.5.1 SDLC y derivados

IBM desarrolló el protocolo Synchronous Data Link Control (SDLC) a mediados de los años 70's para su uso en ambientes SNA (System Network Architecture). SDLC fue el primero de un importante conjunto de protocolos de capa de enlace basados en una operación síncrona y orientada a bit.

Después del desarrollo de SDLC, IBM sometió el protocolo a varios comités de estandarización. La ISO modificó el protocolo para crear HDLC (High Level Data Link Control); la ITU-T posteriormente modificó HDLC para crear LAP (Link Access Control), y después LAPB (Link Access Control Balanced). La IEEE modificó HDLC para crear el estándar 802.2.

SDLC permanece como el principal protocolo de capa de enlace para redes WAN en ambientes SNA.

##### 4.5.1.1 Topologías

SDLC soporta una variedad de tipos de enlace y topologías. Este puede ser usado en enlaces punto a punto y multipunto, medios definidos o no definidos, facilidades de transmisión half o full duplex, y redes de conmutación de paquetes o de circuitos.

SDLC soporta dos principales tipos de estaciones:

- **Primaria.**- Controla la operación de otras estaciones (llamadas secundarias). La estación primaria censa a las estaciones secundarias en un orden predeterminado. Las estaciones secundarias con datos a transmitir entonces pueden acceder al medio de transmisión. La estación primaria también establece o tira conexiones de enlace y administra la conexión de enlace mientras esta en estado operacional.
- **Secundaria.**- Son controladas por las estaciones primarias. Las estaciones secundarias sólo pueden transmitir información a las estaciones primarias, pero sólo bajo permiso de la estación primaria.

Las estaciones primarias y secundarias pueden conectarse en cuatro configuraciones básicas:

- **Punto a punto.** Involucra sólo dos nodos, un primario y un secundario.
- **Multipunto.** Involucra un nodo primario y dos o más nodos secundarios.

- Loop (aro). Involucra una topología en forma de anillo, con el nodo primario conectado al primero y al último nodo secundario. Los nodos secundarios pasan los mensajes de otros nodos para establecer comunicación con el nodo primario.
- Hub go ahead. Involucra un canal de entrada y un canal de salida. El nodo primario usa el canal de salida para comunicarse con los nodos secundarios. Los nodos secundarios usan el canal de entrada para comunicarse con el nodo primario.

Los enlaces SDLC soportan varios tipos de medios de transmisión, tales como líneas telefónicas, fibra óptica, enlaces de microondas, coaxial, y otros.

#### 4.5.1.2 Formato de la trama de SDLC

La trama de SDLC consta de los siguientes campos:

Flag	1 byte que delimita el inicio y el fin de la trama y que se compone de la siguiente secuencia de bits 01111110. Otro patrón de bits consiste en un número entre siete y quince unos consecutivos e indica una función de "abort" (interrupción de trama); lo utiliza el dispositivo transmisor para abortar una trama que ya había comenzado a transmitir.
Address	1 ó 2 bytes que contienen siempre la dirección del nodo secundario involucrado en la actual comunicación. Debido a que el nodo primario siempre es la fuente o destino de la comunicación, no hay necesidad de incluir la dirección del nodo primario. (esta es ya conocida por todos los nodos secundarios).
Control	1 ó 2 bytes. El campo de control usa tres diferentes formatos, dependiendo del tipo de frame SDLC usado: <b>Tramas de información:</b> Estos tipos de frame transportan información de capas superiores. Las secuencias de envío y recepción, así como el bit poll/final (P/F) desempeñan los controles de flujo y de error. El número de secuencia de envío se refiere al número del siguiente frame a enviarse, el número de secuencia de recepción se refiere al número del siguiente frame por recibirse. Las secuencias de envío y recepción son mantenidas por el transmisor y el receptor. El nodo primario usa el bit P/F para indicarle al nodo secundario cuando se requieren su respuesta inmediata. El nodo secundario usa el bit P/F para indicar cuando el actual frame es el último en su actual respuesta. <b>Tramas de supervisión:</b> Estas tramas proveen información de control, solicitan y suspenden transmisiones, reportan el estado y dan el acuse de recibido de los tramas de información. Estas tramas no tienen el campo de información. <b>Tramas sin numeración:</b> Estas tramas no son secuenciadas y son usados con propósitos de control, por ejemplo para inicializar a los nodos secundarios. Dependiendo de las funciones de las tramas no numeradas, el campo de control es de 1 o dos bytes. Algunas tramas no numeradas poseen el campo de información.
Data	Contiene la información de capas superiores
Frame Check Sequence (FCS)	Este campo de 2 bytes es usualmente un cálculo sobre los campos Address, Control, y Data con un algoritmo del tipo Cyclic Redundance Check (CRC). Este calculo es hecho también por el receptor y comparado con el incluido en la trama. Si existe alguna diferencia se asume un error en la trama.

TESIS CON FALLA DE ORIGEN

Tamaño del campo en bytes:

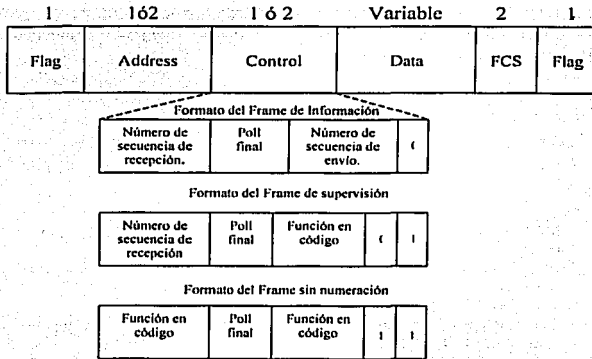
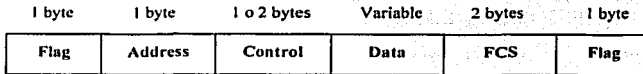


Figura 4.5.1.2.1 Formato de la trama SDLC

#### 4.5.1.3 SDLC bit-stuffing.

Un proceso llamado bit-stuffing es usado para que el patrón del campo Flag no se repita en el resto de la trama. Cuando un frame es transmitido, la trama es revisada en su composición de unos y ceros, de tal forma que siempre que encuentre 5 unos consecutivos insertará un cero después de estos. Así en toda información entre las banderas de inicio y fin de la trama, se insertará un cero después de 5 unos consecutivos.

Del lado del receptor, una vez que se ha reconocido la bandera de inicio, este quitará cada cero encontrado después de 5 unos consecutivos.



RESERVA CON  
 DE ORIGEN



---

#### 4.5.1.4 Modos de operación.

Un nodo secundario puede estar trabajando en un momento dado en cualquiera de los siguientes modos de operación:

**Normal Response Mode (NRM):** En este modo el nodo secundario sólo puede transmitir en respuesta a una petición del nodo primario.

**Asynchronous Response Mode (ARM):** En este modo la estación secundaria puede transmitir un frame sin que este se haya requerido por la estación primaria.

**Asynchronous Balanced Mode (ABM):** En este modo cualquier nodo puede iniciar la transmisión, es decir, todos los nodos tienen igual jerarquía.

**Normal Disconnected Mode:** En este modo el nodo secundario es desconectado lógicamente del enlace. En este modo el nodo secundario no puede recibir o transmitir tramas, con excepción de ciertas tramas de control.

**Modo de inicialización:** Antes de entrar en operación, un nodo secundario se encuentra en modo de inicialización.

**Station's Response Opportunity.** Identifica las condiciones que deben existir para permitir a una estación transmitir.

#### 4.5.2 HDLC.

HDLC (High Level Link Protocol) comparte el mismo frame y funcionalidades que SDLC, sólo difiere en los siguientes aspectos:

- HDLC tiene la opción de un CRC de 32 bits,
- HDLC no soporta las configuraciones tipo loop y hub go ahead. Y,
- HDLC soporta tres modos de transferencia.

Los tres modos de transferencia son los siguientes que ya han sido mencionados en SDLC:

**Normal Response Mode (NRM):** El modo de respuesta normal es un modo de funcionamiento en el que la estación secundaria puede iniciar la transmisión solo si recibe permiso explícito para hacerlo desde la estación primaria.

**Asynchronous Response Mode (ARM):** Es un modo de funcionamiento en el que la estación secundaria puede inicializar una transmisión sin necesidad de recibir permiso explícito por parte de la estación primaria. Este modo ofrece funcionamiento dúplex integral en un enlace punto a punto. Puede considerarse que cada uno de los extremos del enlace está formado por una estación primaria y/o una estación secundaria.

**Asynchronous Balanced Mode (ABM):** En este modo todos los nodos pueden actuar como nodos primarios o nodos secundarios dependiendo de la situación, aquí cualquier nodo puede iniciar la transmisión de información sin necesidad de permisos de cualquier otro nodo.

#### 4.5.3 LAPB.

LAPB es mejor conocido por su presencia en la pila de protocolos X.25. LAPB comparte el mismo formato, tipos de frame y funciones que SDLC y HDLC, aunque LAPB esta restringido al modo de transferencia Asynchronous Balanced Mode. Cualquier estación puede iniciar la transferencia de información.

---

#### 4.5.4 PPP.

El protocolo PPP proporciona un método estándar para transportar datagramas-multiprotocolo sobre enlaces simples punto a punto entre dos "pares" (a partir de aquí, y hasta el final de este punto, utilizaremos el término "par" para referirnos a cada una de las máquinas en los dos extremos del enlace).

Estos enlaces proveen operación bidireccional full dúplex y se asume que los paquetes serán entregados en orden.

Tiene tres componentes:

1. Un mecanismo encapsulación de data gramas multiprotocolo y manejar la detección de errores.
2. Un protocolo de control de enlace (**LCP**, *Link Control Protocol*) para establecer, configurar y probar la conexión de datos.
3. Una familia de protocolos de control de red (**NCPs**, *Network Control Protocols*) para establecer y configurar los distintos protocolos de nivel de red. Funcionamiento general

Para dar un panorama inicial del funcionamiento de este protocolo en el caso en que un usuario de una PC quiera conectarse temporalmente a Internet, describiremos brevemente los pasos a seguir:

En primera instancia, la PC llama al módem del enrutador del **ISP** (*Internet Service Provider*, proveedor del servicio de Internet), a través de un módem local conectado a la línea telefónica.

Una vez que el módem del enrutador ha contestado el teléfono y se ha establecido una conexión física, la PC manda al enrutador una serie de paquetes LCP en el campo de datos de uno o más marcos PPP (esto será explicado con mayor detalle más adelante). Estos paquetes y sus respuestas seleccionan los parámetros PPP por usar.

Una vez que se han acordado estos parámetros se envían una serie de paquetes NCP para configurar la capa de red.

Típicamente, la PC quiere ejecutar una pila de protocolos TCP/IP, por lo que necesita una dirección IP. No hay suficientes direcciones IP para todos, por lo que normalmente cada ISP tiene un bloque de ellas y asigna dinámicamente una a cada PC que se acaba de conectar para que la use durante su sesión. Se utiliza el NCP para asignar la dirección de IP.

En este momento la PC ya es un *host* de Internet y puede enviar y recibir paquetes IP. Cuando el usuario ha terminado se usa NCP para destruir la conexión de la capa de red y liberar la dirección IP, luego se usa LCP para cancelar la conexión de la capa de enlace de datos.

Finalmente la computadora indica al módem que cuelgue el teléfono, liberando la conexión de la capa física.

PPP puede utilizarse no solo a través de líneas telefónicas de discado, sino que también pueden emplearse a través de SONET o de líneas HDLC orientadas a bits.

##### 4.5.4.1 Configuración básica

Los enlaces PPP son fáciles de configurar. El estándar por defecto maneja todas las configuraciones simples. Se pueden especificar mejoras en la configuración por defecto, las cuales son automáticamente comunicadas al "par" sin la intervención del operador. Finalmente, el operador puede configurar explícitamente las opciones para el enlace, lo cual lo habilita para operar en ambientes donde de otra manera sería imposible.

Esta auto-configuración es implementada a través de un mecanismo de negociación de opciones extensible en el cual cada extremo del enlace describe al otro sus capacidades y requerimientos.

##### 4.5.4.2 Entramado

La encapsulación PPP provee multiplexamiento de diferentes protocolos de la capa de red sobre el mismo enlace. Ha sido diseñada cuidadosamente para mantener compatibilidad con el hardware mayormente usado.

Sólo son necesarios 8 bytes adicionales para formar la encapsulación cuando se usa dentro del entramado por defecto. En ambientes con escaso ancho de banda, el entramado puede requerir menos bytes.

El formato de la trama completa es:

Indicador (1 byte)	Dirección (1 byte)	Control (1 byte)	Protocolo (1 o 2 bytes)	Información (variable)	Suma (2 o 4 bytes)	Indicador (1 byte)
-----------------------	-----------------------	---------------------	----------------------------	---------------------------	-----------------------	-----------------------

Todas las tramas comienzan con el byte indicador "01111110". Luego viene el campo dirección, al que siempre se asigna el valor "11111111". La dirección va seguida del campo de control, cuyo valor predeterminado es "00000011". Este valor indica un marco sin número ya que PPP no proporciona por omisión transmisión confiable (usando números de secuencia y acuses) pero en ambientes ruidosos se puede usar un modo numerado para transmisión confiable. El penúltimo campo es el de suma de comprobación, que normalmente es de 2 bytes, pero puede negociarse una suma de 4 bytes. La trama finaliza con otro byte indicador "01111110".

<b>Campo protocolo</b>	<p>Este campo es de 1 o 2 bytes y su valor identifica el contenido del datagrama en el campo de información del paquete (cuando hablamos de "paquete" nos estamos refiriendo a la trama de la capa de enlace, que es en la que opera el PPP; no debe confundirse con los de la capa de red, manejados por IP). El bit menos significativo del byte menos significativo debe ser 1 y el bit menos significativo del byte más significativo debe ser 0. Las tramas recibidas que no cumplan con estas reglas deben ser tratadas como irreconocibles.</p> <p>Los valores en el campo de protocolo dentro del rango de 0hex a 3hex identifican el protocolo de capa de red de los paquetes específicos, y valores en el rango de 8hex a Bhex identifican paquetes pertenecientes al protocolo de control de red asociado (NCPs). Los valores en el campo de protocolo dentro del rango de 4hex a 7hex son usados para protocolos con bajo volumen de tráfico, los cuales no tienen asociados NCP. Valores en el rango de Chex a Fhex identifican paquetes de los protocolos de control de la capa de enlace (como LCP).</p>
<b>Campo información</b>	<p>Puede tener 0 o más bytes. Contiene el datagrama para el protocolo especificado en el campo protocolo. La máxima longitud para este campo, incluyendo el relleno pero no incluyendo el campo de protocolo, es determinada por la unidad máxima de recepción (MRU), la cual es de 1500 bytes por defecto. Mediante negociaciones, PPP puede usar otros valores para la MRU.</p> <p>A la información se le puede agregar un relleno, con un número arbitrario de bytes, hasta llegar a la MRU.</p>

#### 4.5.4.3 Operación del PPP

Para establecer comunicaciones sobre un enlace punto a punto cada extremo debe enviar primero paquetes LCP para configurar el enlace de datos. Después de que éste ha sido establecido, el "par" debe ser autenticado. Entonces, PPP debe enviar paquetes NCP para elegir y configurar uno o más protocolos de red. Una vez que han sido configurados cada uno de los protocolos de la capa de red elegidos, los datagramas de

cada protocolo de capa de red pueden ser enviados a través del enlace. El enlace permanecerá configurado para la comunicación hasta que una serie de paquetes NCP o LCP cierren la conexión, o hasta que ocurra un evento externo (por ej., que un *timer* de inactividad expire o que se produzca una intervención del administrador de la red).

#### 4.5.4.4 Fases de la operación

El procedimiento típico de conexión es el siguiente (ver figura 4.5.4.4.1):

- La PC llama al modem del enrutador del proveedor a través de un modem.
- El modem del enrutador contesta y establece una conexión física.
- El PC y el enrutador intercambian una serie de paquete LCP para seleccionar los parámetros PPP por usar.
- Se envía una serie de paquetes NCP para configurar la capa de red.
- Se asigna al PC una dirección IP a través de NCP para IP.
- El enlace continua configurado para comunicaciones, hasta que LCP, NCP, o algún evento externo lo tire.
- Se usa NCP para dismantelar la conexión en la capa de red y liberar la dirección IP.
- Se usa LCP para eliminar la conexión a nivel de enlace.
- El modem cuelga liberando la capa física.

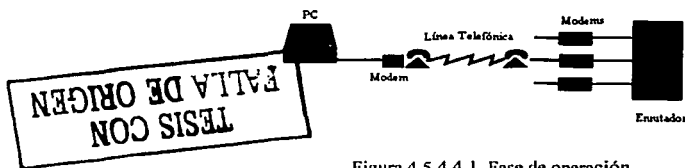


Figura 4.5.4.4.1. Fase de operación

#### 4.5.4.5 Fase de enlace muerto (capa física no lista).

El enlace comienza y termina necesariamente en esta fase. Cuando un evento externo (como una detección de portadora) indica que la capa física está lista para ser usada, PPP procederá con la fase de establecimiento del enlace.

Típicamente, si se utiliza un módem, el enlace volverá a esta fase automáticamente después de la desconexión del mismo. En el caso de un enlace *hard-wired* esta fase puede ser extremadamente corta, tan solo basta detectar la presencia del dispositivo.

#### 4.5.4.6 Fase de establecimiento del enlace.

El protocolo de control de enlace (LCP) es usado para establecer la conexión a través de un intercambio de paquetes de configuración. Este intercambio está completo y se ingresa en el estado abierto de LCP una vez que un paquete de "reconocimiento de configuración" ha sido enviado y recibido por ambos.

Todas las opciones de configuración son asumidas con sus valores por defecto a menos que sean alteradas por un intercambio de paquetes de configuración.

Es importante notar que solo las opciones de configuración que son independientes de cada protocolo particular de capa de red son manejadas por el LCP. La configuración de los protocolos de capa de red individuales es manejada por separado por los protocolos de control de red (NCPs) durante la fase de red.

---

Cualquier paquete que no sea LCP recibido durante esta fase debe ser descartado.

#### **4.5.4.7 Fase de validación.**

En algunos enlaces puede ser deseable solicitar al "par" que se autentifique a sí mismo antes de permitir el intercambio de paquetes del protocolo de capa de red.

Por defecto, la validación o autenticación no es obligatoria. Si una implementación desea que el "par" se autentifique con algún protocolo de validación específico, entonces ésta debe solicitar el uso del protocolo de autenticación durante la fase de establecimiento del enlace.

La autenticación debe tomar lugar tan pronto como sea posible después del establecimiento del enlace.

El progreso de la fase de autenticación a la fase de red no debe ocurrir hasta que la autenticación haya sido completada. Si ésta falla, el que realiza la autenticación debe proceder a la fase de terminación del enlace.

Durante esta fase, sólo son permitidos paquetes del protocolo de control de enlace, el protocolo de autenticación y el monitoreo de calidad de enlace. Cualquier otro paquete recibido debe ser descartado.

La autenticación debe proporcionar algún método de retransmisión, y se procederá a la fase de terminación del enlace sólo luego de que se ha excedido cierta cantidad de intentos de autenticación.

#### **4.5.4.8 Fase de red.**

Una vez que el PPP finalizó las fases anteriores, cada protocolo de capa de red (como por ejemplo IP, IPX o AppleTalk) debe ser configurado separadamente por el protocolo de control de red (NCP) apropiado.

Cada NCP debe ser abierto y cerrado de a uno por vez.

#### **4.5.4.9 Fase abierta.**

Una vez que un NCP ha alcanzado el estado abierto, PPP transportará los correspondientes paquetes del protocolo de capa de red. Cualquier paquete recibido mientras su NCP no esté en el estado abierto debe ser descartado.

Durante esta fase el tráfico del enlace consiste en cualquier combinación posible de paquetes LCP, NCP, y de protocolo de capa de red.

#### **4.5.4.10 Fase de terminación del enlace.**

PPP puede terminar el enlace en cualquier momento. Esto puede ocurrir por la pérdida de la señal portadora, una falla de autenticación, una falla de la calidad del enlace, la expiración de un *timer*, o un cierre administrativo del enlace.

LCP es usado para cerrar el enlace a través de un intercambio de paquetes de "terminación". Cuando el enlace ha sido cerrado, PPP informa a los protocolos de capa de red así ellos pueden tomar la acción apropiada.

Después del intercambio de paquetes de "terminación", la implementación debe avisar a la capa física que desconecte la línea para forzar la terminación del enlace, particularmente en el caso de una falla de autenticación. El que envía una "solicitud de terminación" debe desconectarse después de recibir un "reconocimiento de terminación", o después de que expire el *timer* correspondiente. El receptor de una "solicitud de terminación" debe esperar al "par" para desconectarse, y no lo debe hacer hasta que al menos haya pasado cierto tiempo de reiniciado después de enviar el "reconocimiento de terminación". PPP procederá entonces con la fase de enlace muerto (ver figura 4.5.4.10.1).

**TESIS CON FALLA DE ORIGEN**

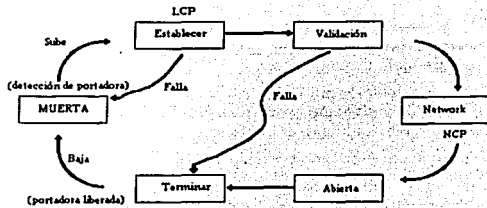


Figura 4.5.4.10.1. Fases en las que puede ser terminada la conexión

Cualquier paquete recibido durante esta fase que no sea LCP debe ser descartado.

La clausura del enlace por LCP es suficiente. No es necesario que cada NCP envíe paquetes de terminación. A la inversa, el hecho de que un NCP sea cerrado no es razón suficiente para causar la terminación del enlace PPP, aún si ese NCP era el único actualmente en el estado abierto.

#### 4.5.4.11 Negociación automática de opciones

La negociación de opciones es definida por eventos, acciones y transiciones de estados. Los eventos incluyen la recepción de comandos externos (como apertura y clausura), expiración de *timers*, y recepción de paquetes de un "par". Las acciones incluyen el arranque de *timers* y la transmisión de paquetes al "par".

Algunos tipos de paquetes ("no reconocimientos de configuración", "rechazos de configuración", "solicitudes de eco", "respuestas de eco", etc.) no son diferenciados aquí ya que producen siempre las mismas transiciones.

<b>Estados</b>	Algunos posibles estados son: "inicial" (la capa más baja no está disponible y no ha ocurrido una apertura), "starting" (ha sido iniciada una apertura pero la capa más baja aún no está disponible), "closed" (el enlace está disponible pero no ha ocurrido una apertura), etc.
<b>Eventos</b>	Las transiciones y las acciones en la negociación son causadas por eventos. Algunos son: "up" (este evento ocurre cuando la capa más baja indica que está lista para transportar paquetes; típicamente es usado por los procesos de manejo y llamada de un módem, y también puede ser utilizado por el LCP para indicar a cada NCP que el enlace está entrando en la fase de red). Otro evento muy común es "down" (cuando la capa más baja indica que ya no está lista para transportar paquetes, este evento también es generalmente utilizado por un módem o por un LCP).
<b>Acciones</b>	Son causadas por eventos y habitualmente indican la transmisión de paquetes y/o el comienzo o parada de <i>timers</i> . Algunas acciones son: "evento ilegal" (esto indica acerca de un evento que no puede ocurrir en una negociación implementada correctamente), "capa hacia arriba" (esta acción indica a las capas superiores que la negociación está entrando en estado "abierto"; típicamente es utilizada por el LCP para indicar el evento "up" a un NCP, por un protocolo de autenticación, o de calidad de enlace).
<b>Prevención</b>	El PPP intenta evitar ciclos mientras se efectúa la negociación de opciones de configuración. De todas formas, el protocolo no garantiza que no ocurrirán ciclos. Como en cualquier

de ciclos	negociación es posible configurar dos implementaciones PPP con políticas conflictivas que nunca converjan finalmente. También es posible configurar políticas que converjan, pero que se tomen un tiempo significativo para hacerlo.
Timers	Existen distintos tipos de <i>timers</i> . Por ejemplo, el " <i>timer</i> de reiniciado" es utilizado para controlar el tiempo de las transmisiones de solicitud de configuración y los paquetes de solicitud de terminación. La expiración de este <i>timer</i> causa un evento de "tiempo cumplido" y la retransmisión de la correspondiente "solicitud de configuración" o el paquete de "solicitud de terminación". Este <i>timer</i> debe ser configurable, pero por defecto durará 3 segundos. Este tiempo está pensado para bajas velocidades, como las líneas telefónicas típicas.  Otro ejemplo de <i>timer</i> es el de "terminación máxima", que es un contador de reiniciado requerido para las solicitudes de terminación. Indica el número de paquetes de "solicitudes de terminación" enviados sin recibir un "reconocimiento de terminación". Debe ser configurable pero por defecto se establece en 2 transmisiones.

#### 4.5.5 Anchos de banda en WAN's

El ancho de banda en el cableado de cobre que se provee en Norte América y en muchas otras partes del mundo es por medio de la Jerarquía Digital de Norte América o estándar americano, el cual se muestra en la siguiente tabla. Un canal en este tipo de jerarquía es llamado DS (Digital Stream). Los DS's son multiplexados juntos para una alta velocidad en los circuitos WAN. Los DS-1 y DS-3 son las capacidades más usadas comúnmente.

Señal	Capacidad	Numero de DS	Nombre Coloquial
DS-0	64 kbps	1	Canal
DS-1	1.544 Mbps	24	T1
DS-1C	1.544 Mbps	24	T1C
DS-2	6.312 Mbps	64	T2
DS-3	44.736 Mbps	272	T3
DS-4	274.176 Mbps	1032	T4

TESIS CON  
 FALLA DE ORIGEN

Para Europa el estándar es diferente. El Comité de Telefonía y Postal Europeo (CEPT) ha definido una jerarquía llamada E system, que se muestra en la siguiente tabla:

**TESTES CON FALLA DE ORIGEN**

Señal	Capacidad	Numero de E1's
E0	64 Kbps	N/A
E1	2.048 Mbps	1
E2	8.448 Mbps	4
E3	34.368 Mbps	16
E4	139.264 Mbps	64

SDH (Synchronous Digital Hierarchy) es un estándar internacional para transmisión de datos sobre fibra óptica. SDH define un estándar básico de transmisión que es de 51.84 Mbps, que también es conocido con el nombre de STM-0, las velocidades de transmisión superiores que ofrece este estándar son múltiplos de la velocidad básica de transmisión. Las velocidades del estándar STS-1 son los niveles establecidos para SONET, y también existen los niveles de transmisión llamados OC (Optical Carrier- levels).

A continuación se muestra una tabla con sus respectivos valores y equivalencias

Nivel STM	Nivel STS	Nivel OC	Velocidad de transmisión
STM-0	STS-1	OC-1	51.84 Mbps
STM-1	STS-3	OC-3	155.52 Mbps
STM-4	STS-12	OC-12	622.08 Mbps
	STS-24	OC-24	1244 Gbps
STM-16	STS-48	OC-48	2488 Gbps
	STS-96	OC-96	4976 Gbps
STM-64	STS-192	OC-192	9952 Gbps

**4.5.6 Tecnologías para el establecimiento de conexiones usando enlaces conmutados**

**4.5.6.1 Red telefónica**

Los servicios telefónicos regulares o también conocidos como (POTS) o antiguo plan de servicio telefónico, fue diseñado para la carga de tráfico de voz en forma analógica utilizando par de cobre como medio de transmisión. Por otra parte, las computadoras trabajan por medio de dígitos y a su vez se comunican digitalmente. Para poder realizar la comunicación digital sobre un medio de transmisión que fue diseñado para transportar la información en forma analógica, es necesaria que esta información digitalizada sea transformada a una señal analógica. Esto objetivo se logra por medio de un módem (modulador-demodulador) el cual convierte la señal digital en señal analógica y viceversa. De esta manera se utiliza la vieja red telefónica para la transmisión de datos entre estaciones de trabajo. Claro que este tipo de recurso tiene desventajas debido a las interferencias electromagnéticas y ruido que existe en el medio transmisión,



además del desgaste que pudiera tener el mismo, este tipo de factores son capaces de alterar la señal que contiene la información y provocar errores en la información que se esta enviando por medio de esta red (ver figura 4.5.6.1.1).

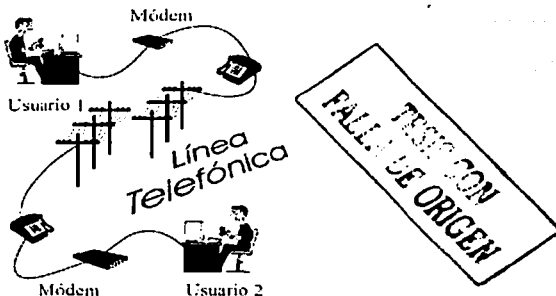


Figura 4.5.6.1.1. Conexión por medio de la Red telefónica

#### 4.5.6.2 ISDN (Red Digital de Servicios Integrados).

##### 4.5.6.2.1 Definición de la Red Digital de Servicios Integrados (ISDN).

ISDN (Integrated Services Digital Network, que ya traducido significa, Red Digital de Servicios Integrados, RDSI) se define como una evolución de las Redes actuales, que permite una conexión de extremo a extremo a nivel digital ofreciendo diferentes servicios. Permite la transferencia de información entre cualquier usuario de la propia Red. Al ser una Red Digital permite integrar señales analógicas, mediante la transformación Analógico - Digital, y digitales, en base a esto se ofrece un nivel básico de comunicación de 64 Kbps. La integración de diferentes servicios está asegurada debido a la estructura digital de la propia Red, ya que las señales Digitales se transforman de código y las Analógicas, mediante técnicas de muestreo, se digitalizan para su envío posteriormente.

En la figura 4.5.6.2.1.1 podemos observar un ejemplo de la integración de las diferentes señales mencionadas en la ISDN.

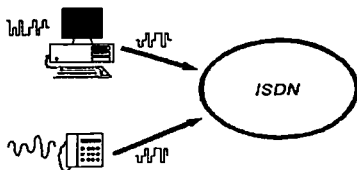


Figura 4.5.6.2.1.1. Integración de señales en ISDN.

Como se puede observar, en el caso de comunicaciones analógicas (voz), el teléfono efectúa la conversión Analógico Digital. En el caso de equipos digitales, se transforma el código original a otro más adecuado a la comunicación (Transformación de código).

#### 4.5.6.2.2 Generalidades de ISDN

ISDN presenta al usuario una serie de interfaces normalizadas para la conexión a la Red. De esta forma se pretende normalizar todas las conexiones a la Red mediante los Accesos de Usuario (interface estándar de conexión a la Red Digital de Servicios Integrados)

La diferencia fundamental entre los diferentes Accesos definidos es la capacidad de información que son capaces de gestionar.

Los Accesos a velocidades superiores a 2 Mbps (acceso primario) se engloban en la ISDN de Banda Ancha y se definen según la Jerarquía de Transmisión Digital o en el modo de transferencia asíncrono (ATM).

#### 4.5.6.2.3 Centrales ISDN

La Central Pública ISDN se define, al igual que la Red, como la evolución de las Centrales Públicas de Conmutación de la RDI (Red Digital Integrada) permiten la conmutación de circuitos a 64 Kbps.

La evolución en las técnicas de conmutación y transmisión, de analógicas a digitales, han permitido el desarrollo de la ISDN, digitalizando la comunicación extremo a extremo.

En la figura 4.5.6.2.3.1 podemos observar la evolución de la Red con la introducción de las técnicas digitales.

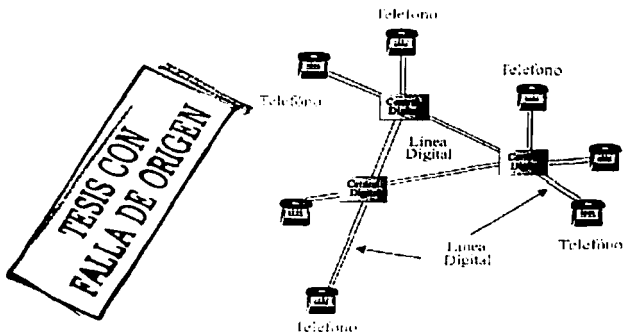


Figura 4.5.6.2.3.1 Evolución de la red de Conmutación.

Una Central Pública se considera ISDN cuando cumple los requisitos enumerados a continuación:

Tanto la matriz de conmutación de circuitos como el sistema de transmisión entre centrales debe ser digital, Centrales RDI.

La señalización requerida para ISDN entre Centrales Públicas se basa en el Sistema de Señalización por Canal Común No. 7 del CCITT. (SSCC 7). Un sistema basado en intercambio de información mediante mensajes entre Centrales.

---

La central debe estar utilizar señalización PUSI (Parte Usuario Servicio Integrado), que se encarga de dar servicio a los diferentes Accesos de Usuario de la ISDN de forma especializada. Además de contar con la señalización PUT (Parte Usuario Telefónico), encargada de atender las comunicaciones de voz, ancho de banda 3.1 KHz.

Debe disponer de capacidades de conmutación de paquetes, mediante el MP (Manejador de paquetes) o ECP's (Elementos de Conmutación de Paquetes), de forma que los paquetes de información del usuario puedan progresar en la Red. Esta característica no está disponible aún en algunas tecnologías de forma que en algunos Accesos no podrá habilitarse.

#### **4.5.6.2.4 Línea de transmisión**

Se entiende por Línea de Transmisión al medio físico necesario que sirve de soporte al Acceso del Usuario. Se comentan a continuación las características de las líneas para cada Acceso:

**Acceso Básico:** línea de transmisión a dos hilos mediante cable de cobre (igual al empleado en la RTPC). Gracias a los códigos de línea empleados, sistemas de reducción del ancho de banda de transmisión, se pueden alcanzar los 5 Km sobre cable de pares de calibre normal. En el caso de excesiva pérdida debido a la distancia se pueden emplear sistemas de regeneración o multiplexores que son capaces de multiplexar 12 Accesos Básicos en una trama a 2 Mbps.

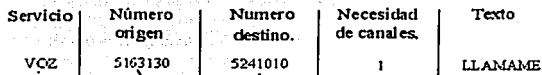
**Acceso Primario:** la línea de transmisión estará formada por dos pares de hilos o por fibra óptica. En el caso de Clientes que posean fibra óptica se tenderá un agregado a 2Mbps para el Acceso. Si el Cliente no posee fibra óptica se emplearán dos pares de cable metálico (cobre), similares a los empleados en el Acceso Básico, mediante unos módem BB (Banda Base) a 2 Mbps se podrá poner en servicio el Acceso.

En cualquier caso el personal de la compañía de explotación del servicio puede seleccionar el medio más adecuado debido a su experiencia y a las características de cada Cliente, aunque sería deseable para el caso de Accesos Primarios la utilización de fibra óptica.

#### **4.5.6.2.5 ISDN de banda estrecha**

Los Accesos de Usuario definidos para ISDN en Banda Estrecha permiten la comunicación a velocidades de 64 Kbps, o agrupaciones de esta velocidad, mediante la Red de Conmutación de las Centrales Públicas. La solicitud de esta comunicación se efectúa mediante mensajes enviados a través de un canal de señalización adicional a cada acceso, bien desde los equipos terminales o desde la Central Pública.

Debido a la estructura de transmisión y conmutación de la ISDN, así como las técnicas digitales, la integridad de la información está asegurada. Lo cual permite comunicaciones secretas o al menos más inmunes a interceptaciones. Por otra parte las técnicas digitales permiten un tratamiento de las señales de forma que la transmisión de la información no sufra degradaciones debido a la distancia o al ruido (ver figura 4.5.6.2.5.1).



VOZ / 5163130 / 5241010 / 1 / "LLAMAME"

0100101001010010101001010010100100101010100100  
1010010 / 010010100101101 / 010101000010101 / 01 /

Transmisión por canal "D".

0 1 0 0 1 0 1

TESIS CON FALLA DE ORIGEN

Figura 4.5.6.2.5.1. Ejemplo de paquete de señalización.

Gracias al tipo de señalización (conmutación de paquetes) el establecimiento de una conexión ISDN se efectúa a más velocidad, lo que permite un ahorro considerable de tiempo en el establecimiento de la comunicación. Es también una ventaja añadida la posibilidad de enviar pequeños mensajes en la "llamada" para indicar situaciones especiales, envío de textos como: "Lláname en 30 minutos", permiten al usuario llamado la posibilidad de devolver la llamada. La aparición de elementos como el número de origen de la llamada, el número destino, etc., mejoran los servicios de la Red en beneficio del Usuario. La anterior figura muestra un ejemplo de un mensaje de señalización.

4.5.6.2.6 Acceso Básico (2B+D)

Denominado Acceso Básico de Usuario o Acceso 2B+D, está formado por:

2B	Dos canales conmutados a 64 Kbps para transferencia de información extremo a extremo en modo digital
1D	Un canal de señalización en modo paquete según el protocolo denominado LAPD (Protocolo de Acceso al Enlace por Canal D en inglés) con una velocidad efectiva de 16 Kbps. Debido a que este canal se mantiene mucho tiempo inactivo se especifica que puede emplearse para informaciones del cliente en modo paquete. (recomendación X.25)

Es posible la utilización de ambos canales B para una misma comunicación, en realidad para Videotelefonía o Videoconferencia se emplean los dos canales de forma simultánea debido a que la utilización de un solo canal B no permite una conexión clara en imagen.

Se pueden emplear Equipos ISDN que demandan mayor capacidad de información, equipos para envío de música de Alta Definición (HiFi) calidad similar al CD o MD, que precisan de 6 canales de comunicación,

para ello se emplean tres Accesos Básicos ( $3 \times 2B = 6$  canales) y el ET del Cliente gestionará las llamadas necesarias en cada Acceso.

#### 4.5.6.2.7 Acceso Primario. (30B+D)

El Acceso Primario o Acceso 30B+D se constituye en la forma siguiente:

<b>30B</b>	30 canales conmutados de velocidad 64 Kbps, para información de Cliente.
<b>1D</b>	Un canal de señalización a 64 Kbps, empleado también para el envío de información en modo paquete.

Como en todo sistema de transmisión digital necesitamos de elementos de sincronización, se añade un canal más a 64 Kbps para la sincronización de trama. De esta forma el Acceso Primario se compone de 32 canales de 64 Kbps ( $32 \times 64 = 2048$  Kbps = 2 Mbps.)

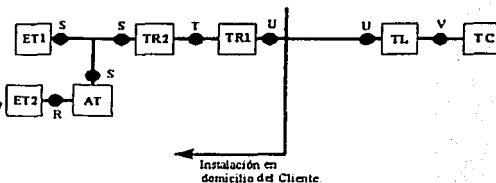
En el Acceso Primario ISDN se permiten además agrupaciones de varios canales para transferencia de información:

<b>Canales 110</b>	6 canales a 64 Kbps, velocidad 384 Kbps.
<b>Canales 112</b>	30 canales a 64 Kbps, velocidad 1920 Kbps.

Es lógico suponer que el Acceso Básico está definido para Clientes o aplicaciones que requieran poca capacidad de transferencia de información, mientras que el Acceso Primario está definido para Clientes con media necesidad de información. Para clientes con gran capacidad de información se hará necesaria la utilización de Accesos en Banda Ancha.

#### 4.5.6.2.8 Configuración de referencia

La configuración de referencia está definida por Agrupaciones funcionales, equipos con una función específica y puntos de referencia o interfaces, puntos definidos en los que la ISDN presenta características de transmisión o conmutación determinadas (ver figura 4.5.6.2.8.1).



□ Agrupación Funcional.

● Punto de Referencia o Interfaz.

Figura 4.5.6.2.8.1. Configuración de Referencia.

A continuación se especifican las características de cada elemento.

#### 4.5.6.2.9 Agrupaciones funcionales

Las agrupaciones funcionales son elementos que desarrollan una función, en este caso corresponden a equipos o elementos del mismo Cliente o Central.

##### TC Terminación de Central

- Situada en la Central de Conmutación.
- Se encarga del mantenimiento del Acceso de Usuario.
- Realiza la conexión de canales.
- Soporta la señalización del usuario y el envío de información en modo paquete.

##### TL Terminación de Línea

- Situada en la Central.
- Se encarga de los aspectos de transmisión.
- Convierte el código binario al código de línea empleado.
- Controla la sincronización del Acceso.
- Ésta agrupación funcional está unida a la TC formando una agrupación.

##### TRI Terminación de Red No.1

- Es el primer elemento en el domicilio del Cliente y obligación de la compañía que imparte el servicio.

- Este equipo permite la sincronización de los diferentes equipos conectados a continuación, así como el establecimiento de secuencias de prueba con la central. Su misión más importante es la de adaptar las señales existentes en la línea a las señales definidas en los interfaces S o T.
- En el Acceso Básico los equipos terminales de Cliente se conectan al TR1 mediante una configuración denominada Bus Pasivo. A este Bus acceden solo y exclusivamente equipos ISDN en número máximo de ocho. Los terminales no ISDN se conectarán a través de su correspondiente Adaptador de Terminales y estos a su vez se conectarán al Bus. Contando pues el número de adaptadores y de equipos ISDN no se puede superar el número máximo de ocho equipos en el Bus.
- En el Acceso Básico la TR1 deberá estar conectada, ya que es el elemento encargado de dar alimentación a los equipos terminales. Si la alimentación del edificio se interrumpiera sería la Central la que telcalimentará al TR1 y a un solo equipo terminal que deberá estar programado como emergencia, esto permite la utilización del Acceso aunque no tengamos alimentación.
- Estas consideraciones no son de aplicación al Acceso Primario, ya que por regla general este estará formado por equipos de transmisión que deben obtener la energía de forma local.
- Permite la verificación a distancia, pudiéndose evaluar la calidad del enlace.

#### **BUS Pasivo**

- Lo definimos como la instalación necesaria en el domicilio del Cliente para la conexión de los equipos terminales al Acceso. Existen dos diferentes categorías de Buses, las de larga distancia (Buses Largos) y las de corta distancia (Buses Cortos), cada una de estas categorías se divide en dos diferentes instalaciones en función de las necesidades puntuales de cada Usuario.
- El Bus pasivo debe estar presente en todas las instalaciones de Usuario de la ISDN. En ningún caso se conectarán equipos directamente al TR1 ya que esto puede afectar a las características de transmisión del Acceso impidiendo un correcto funcionamiento del mismo.

#### **TR2 Terminación de Red No. 2**

- Realiza funciones de control en la instalación del Cliente.
- Tratamiento de la señalización.
- Multiplexación de canales de información.
- Conmutación local.
- Concentración de tráfico y mantenimiento de la instalación del usuario.

#### **ET1 Equipo Terminal No. 1**

- Es el Equipo Terminal ISDN.
- Preparado para señalización en modo paquete y gestión de canales de información.
- Algunos ejemplos pueden ser Teléfonos ISDN, equipos de Videotelefonía, Tarjetas de PC, etc.

#### **AT Adaptador de Terminales**

- Equipo ISDN que tienen la capacidad de adaptar interfaces.
- Convierte las señales de otros equipos no ISDN a señales adecuadas al interface correspondiente (interface "S").

## ET2 Equipos Terminales No. 2

- Equipos no ISDN que pueden conectarse mediante una interface no Normalizado por ISDN a la Red Fax Grupos 2 y 3, Teléfonos analógicos, módem.

### 4.5.6.2.10 Puntos de referencia o interfaces

Los Puntos de Referencia son interfaces entre las agrupaciones funcionales y pueden ser Reales o Virtuales. Los puntos de referencia Virtuales no son accesibles, o en algunos casos coinciden con otra interface.

Puntos de referencia	Funciones
V	<ul style="list-style-type: none"><li>Separación entre las funciones de conmutación y transmisión en la Central</li><li>Interface Virtual ya que TL y TC están unidas en la Placa de Línea de la Central Pública.</li></ul>
U	<ul style="list-style-type: none"><li>Características de transmisión en la línea</li><li>Especifica el formato de la trama en la misma, los códigos posibles, niveles de señal, las perturbaciones permitidas (atenuación, ruido)</li><li>Brinda al TR1 la posibilidad sincronización, la activación y sirve de transporte al Acceso</li></ul>
T	<ul style="list-style-type: none"><li>Separación entre la transmisión de línea y la transmisión en el domicilio del Cliente</li><li>Es un punto de Transmisión que puede coincidir con el Punto "S".</li></ul>
S	<ul style="list-style-type: none"><li>Interface de conexión físico de los equipos terminales ISDN</li><li>Define la estructura de trama, la gestión del Canal D, la sincronización y las características de transmisión.</li></ul>
R	<ul style="list-style-type: none"><li>Interface no normalizada en ISDN</li><li>Contiene un AT para que el equipo correspondiente pueda conectarse al Acceso.</li></ul>

En el Acceso Básico los puntos S y T corresponden a la misma interface, denominándose interface S. Así pues la conexión de un equipo terminal se efectúa directamente al TR1, mediante una configuración de instalación determinada (Bus). Puede conectarse un TR2 pero éste deberá implementar una interface S para la conexión.

En el Acceso Primario se conecta un TR2 para transformar la interface T en una interface S permitiendo la conexión de equipos terminales ISDN. En el caso de equipos que gestionen los 30 canales de comunicación, Videoconferencia de alta calidad, este se conecta a la interface T, ya que el equipo hará las funciones de TR2.

En el lado de Central las agrupaciones TL y TC están siempre incluidas en la correspondiente tarjeta de línea, así pues la interface V no será accesible. La interface U puede adaptarse a otras señales mediante los equipos de transmisión adecuados, de esta forma se asegura una cobertura mayor (multiplexores).

### 4.5.6.2.11 Numeración ISDN

La numeración ISDN corresponde a los nuevos Planes de Numeración. De esta forma un número ISDN se direcciona mediante la marcación de un bloque numérico correspondiente a la localidad del destino de la conexión.

El número ISDN está formado por los campos siguientes:



**IP** Indicativo del País (para México 52)  
**IN** Indicativo Nacional

**Número** Denominado SDE o MNA según los siguientes casos:

**MNA** Múltiples números por Acceso, en el caso de Accesos Básicos se pueden asignar hasta un máximo de 8 por Acceso.  
**SIDE** Selección Directa a Extensiones (DID en inglés) Corresponde a un bloque de numeración asignado al Acceso. Sólo para líneas de PBX ISDN.

**Subdirección:** Permite la conexión con un Equipo Terminal determinado del Acceso, funciona como un número adicional dentro del propio Acceso.

Como se puede observar la numeración ISDN consta, sin tener en cuenta la subdirección, de diez dígitos. Esto se adaptará al nuevo Plan de Numeración (8 dígitos)

#### 4.5.6.2.12 Servicios de la ISDN

Se definen a continuación los diferentes servicios que ofrece la ISDN en los diferentes Accesos de Usuario de Banda Estrecha.

##### Servicios portadores

Existen diferentes servicios Portadores englobados en dos categorías diferentes: Servicios Portadores en Modo Circuito y Servicios Portadores en Modo Paquete.

<b>Servicios portadores en modo circuito</b>	<p>Presentan la posibilidad de conexiones a velocidades de 64 Kbps o superiores mediante conmutación de circuitos. Se definen tres servicios en función del tratamiento de la señal digital:</p> <p><i>a) Servicio portador a 64 Kbps sin restricciones</i></p> <p>Se define como el servicio portador que puede emplear uno o varios canales a 64 Kbps, sin ninguna estructura predefinida, de forma que la Central es transparente a la información del usuario. Por extensión del servicio que puede prestar se denomina también servicio portador de Datos.</p> <p><i>b) Servicio portador para conversación</i></p> <p>Se define como el servicio portador que mediante la utilización de un canal a 64 Kbps permite la comunicación de voz extremo a extremo. Está estructurado según la codificación de una señal digitalizada de ancho de banda 4 KHz. Es el servicio de Voz de la ISDN.</p> <p><i>c) Servicio portador 3.1 KHz</i></p> <p>Se define como el servicio portador que emplea un canal de 64 Kbps para intercambio de información con un ancho de banda de 3,1 KHz, desde 300 Hz a 3400 Hz. Necesita de un Adaptador de Terminales. Las señales analógicas pueden generarse en un Fax de Grupo 2, en un módem, en un teléfono analógico, etc.</p>
--	---

	<p>Servicios portadores en modo paquete</p> <p>Permite la explotación del canal D para comunicaciones en modo paquete con otros usuarios de la Red.</p>
Servicios portadores en modo paquete	<p><i>a) Servicio portador en modo paquete virtual</i></p> <p>Se define como el servicio portador en modo paquete que emplea procedimientos de llamada para el establecimiento de la conexión en modo paquete. Su velocidad binaria es de 9600 bps, aunque en algunos casos puede llegar a velocidades similares a la del canal D.</p> <p><i>b) Servicio portador en modo paquete permanente</i></p> <p>Se define así al servicio de conmutación de paquetes exento de las fases de establecimiento de llamada, de esta forma la conexión se efectúa entre dos entidades de conmutación de paquetes de forma permanente y la transferencia de información efectiva supera al servicio anterior, si bien no puede elegirse el destinatario de la información. Aunque la velocidad binaria de transferencia de datos es igual a la del caso anterior, la ausencia de elementos de control de la comunicación permite enviar más información con menos paquetes.</p>

#### 4.5.6.2.13 Teleservicios

Se define como Teleservicio al servicio que utiliza los Servicios Portadores para la interconexión de Equipos Terminales de Cliente. Esta comunicación está regida por unas características especificadas para cada Teleservicio. En cada Teleservicio se comenta el Servicio Portador empleado entre paréntesis.

*a) Telefonía (Audio 3,1 o Conversación)*

Servicio similar al ofrecido por la RTPC

Permite la comunicación de señales vocales con ancho de banda de 300 a 3400 Hz. Interfuncionamiento con la RTPC.

*b) Telefonía a 7 KHz (Sin Restricciones)*

Servicio de telefonía mejorada

Similar a las comunicaciones microfónicas

Emplea un ancho de banda de 7 KHz para comunicaciones vocales.

*c) Transmisión de datos (Sin Restricciones)*

Permite la conexión de canales B de forma transparente, sin interferir la información de Usuario

No existe interfuncionamiento con la RTPC.

*d) Fax Grupos 2/3 (Audio 3,1)*

Permite la conexión de datos mediante digitalización de señales analógicas para servicio de fax

Puede emplearse para conexiones de fax con los equipos conectados a la RTPC.

*e) Fax Grupo 4 (Sin Restricciones)*

Servicio de fax definido para ISDN

Permite la conexión de Facsímil de alta calidad sin interfuncionamiento con la RTPC.

*f) Teletex (Audio 3,1)*

Necesita de Adaptadores de Terminales para su conexión a la ISDN.

*g) Videotex (Audio 3.1 o Sin Restricciones)*

Servicio similar al ofrecido por la RTPC

Permite la interconexión con la RTPC, siempre que se emplee un Equipo Terminal RTPC a través de un Adaptador de Terminales.

*h) Videotelefonía (Sin Restricciones)*

Permite la transmisión de imágenes junto con voz en una conexión ISDN extremo a extremo

No es compatible con la RTPC.

*i) Modo Mixto (Sin Restricciones)*

Permite el envío de información combinada, imágenes y texto a través de la ISDN

No es compatible con la RTPC.

Los Teleservicios de Transmisión de Datos y Videotelefonía pueden emplearse con combinaciones de canales B, mediante el empleo de H0 o H12 o de la asociación de dos canales B, comunicación a 128 Kbps.

Existe la posibilidad de que aparezcan nuevos Teleservicios, aunque harán uso de uno de los servicios Portadores comentados.

#### **4.5.6.2.14 Servicios suplementarios.**

Se denominan también Servicios de Valor Agregado y modifican o amplían las características de los Accesos de Usuario en Banda Estrecha. Los principales Servicios Suplementarios son:

*Grupo Cerrado de Usuarios.*

Permite formar grupos de acceso restringido, tanto para llamadas entrantes como salientes.

*Identificación de llamada.*

Permite al usuario llamado la presentación del número de la persona que ha realizado la llamada.

*Restricción de identificación de usuario llamante.*

Permite al usuario que efectúa la llamada restringir su identificación hacia el usuario llamado.

*Identificación de usuario conectado.*

Permite al usuario llamante conocer la identidad del usuario con el que se ha establecido la llamada, en caso de desvíos.

*Restricción de Identificación de usuario conectado.*

Permite al usuario llamado impedir la identificación de la conexión hacia el usuario llamante.

*Llamada en espera.*

Informa al usuario de la presencia de una llamada cuando tiene los dos canales B ocupados.

*Múltiples números por acceso.*

Permite dotar al acceso de varios números, en el caso de Acceso Básico, 8 por acceso.

*Selección directa a extensiones.*

Permite la selección de un usuario conectado a través de un PBX de forma directa, mediante marcación.

*Subdireccionamiento.*

---

Muestra una capacidad adicional para el enrutamiento de una llamada en un acceso, sin consumir recursos de numeración.

#### *Portabilidad de terminales.*

Este servicio suspende una llamada establecida durante un máximo de 3 minutos, desconectando físicamente el terminal de la comunicación. La comunicación así suspendida puede recuperarse desde cualquier otro terminal en el mismo acceso.

#### *Línea directa sin marcación.*

Establece la marcación directa, llamada a un número previamente almacenado sin más que descolgar el microteléfono.

#### *Desvío de llamadas.*

Reenruta una llamada entrante a otro destino predefinido.

#### *Información de costo.*

Permite conocer el costo de la llamada, existen dos modalidades: durante la comunicación y al final de la comunicación.

Estos Servicios Suplementarios son los más comunes, aunque existen dos servicios que aumentan las posibilidades del acceso:

#### *Información Usuario a Usuario nivel 1.*

Permite el intercambio de información entre usuarios en la fase de establecimiento de la llamada.

#### *Información Usuario a Usuario nivel 3.*

Es una ampliación del servicio anterior, permitiendo mensajes de mayor longitud en la misma fase de establecimiento de la llamada.

Se entienda por fase de establecimiento de llamada a todos aquellos paquetes que viajan por el canal D y sirven para el establecimiento de una llamada, el mantenimiento de la misma y la desconexión de la comunicación.

### **4.6 Tecnologías para el establecimiento de conexiones por medio de enlaces vía circuitos virtuales.**

En esta parte del capítulo analizaremos dos tecnologías que nos permiten realizar enlaces por medio de circuitos virtuales. Empezaremos con la tecnología llamada Frame Relay y después continuaremos con la tecnología ATM.

#### **4.6.1 Frame Relay.**

##### **4.6.1.1 Definición.**

Frame Relay es un protocolo de WAN de alto desempeño que opera en las capas físicas y de enlace de datos del modelo de referencia OSI. Originalmente, la tecnología Frame Relay fue diseñada para ser utilizada a través de las ISDN (Interfases de la Red Digital de Servicios Integrados). Hoy en día, se utiliza también a través de una gran variedad de interfases de otras redes.

Frame Relay es un ejemplo de tecnología de conmutación de paquetes. En las redes que utilizan esta tecnología, las estaciones terminales comparten el medio de transmisión de la red de manera dinámica, así como el ancho de banda disponible. Los paquetes de longitud variable se utilizan en transferencias más eficientes y flexibles. Posteriormente, estos paquetes se conmutan entre los diferentes segmentos de la red hasta que llegan a su destino. Las técnicas de multiplexaje estadístico controlan el acceso a la red en una red

---

de conmutación de paquetes. La ventaja de esta técnica es que permite un uso más flexible y eficiente de ancho de banda.

Frame Relay normalmente opera a través de instalaciones WAN que ofrecen servicios de conexión más confiables y un mayor grado de confiabilidad que las disponibles a finales de los años 70, e inicio de los 80, las cuales servían como plataformas habituales para las WAN's X.25. Frame Relay es estrictamente una arquitectura de Capa 2, y resulta apropiada para las aplicaciones WAN actuales, como la interconexión LAN.

#### **4.6.1.2 Estandarización de Frame Relay.**

La propuesta inicial para la estandarización de Frame Relay se presentó el CCITT (Comité Consultivo Internacional de Telefonía y Telegrafía) en 1984. Sin embargo, por su falta de interoperabilidad y estandarización, Frame Relay no tuvo gran aceptación a finales de los 80.

En 1990 ocurrió un gran desarrollo en la historia de Frame Relay cuando las compañías Cisco, Digital Equipment, Northern Telecom y StrataCom formaron un consorcio para aplicarse al desarrollo de la tecnología Frame Relay. Dicho consorcio desarrolló una especificación que conformó el desarrollo básico de Frame Relay que se estaba analizando en el CCITT, pero ampliaba el protocolo con características que ofrecían facilidades adicionales en entornos complejos de interconectividad en redes. A estas extensiones de Frame Relay se les conoce en conjunto como LMI (Interfase de Administración Local).

Desde que la especificación del consorcio se desarrolló y publicó, muchos proveedores han anunciado su apoyo a esta definición extendida de Frame Relay. La ANSI y el CCIT estandarizaron, posteriormente sus propias variaciones a la especificación LMI original, y actualmente se utilizan dichas especificaciones estandarizadas con mayor frecuencia que la versión original.

En el ámbito internacional, la tecnología Frame Relay fue estandarizada por la ITU-T (Unión Internacional de Telecomunicaciones, Sector Telecomunicaciones). En Estados Unidos, Frame Relay es un estándar de ANSI (Instituto Nacional Americano de Estándares).

#### **4.6.1.3 Dispositivos conectados en una red Frame Relay.**

Los dispositivos conectados a una WAN Frame Relay caen dentro de una de dos categorías generales: DTE (Equipo Terminal de Datos). Los DTEs, en general, se consideran equipo de terminal par a una red específica y, por lo general, se localizan en las instalaciones de un cliente. De hecho, pueden ser propiedad del cliente. Algunos ejemplos de los dispositivos DTE son las terminales, computadoras personales, enrutadores y puentes.

Los DCE son dispositivos de interconectividad de redes propiedad de la compañía de larga distancia. El propósito del equipo DCE es proporcionar los servicios de temporización y conmutación en una red, en realidad los dispositivos que transmiten datos a través de la WAN. En la mayoría de los casos, éstos son switches de paquetes. En la figura 4.6.1.3.1 se muestra la relación entre las dos categorías de dispositivos.

La conexión entre un dispositivo DTE y un DCE consta de un componente de la capa física y otro de la capa de enlace de datos. El componente físico define las especificaciones mecánicas, eléctricas y de procedimiento para la conexión entre dispositivos. Una de las especificaciones de interfase de la capa física que más se utiliza es la especificación del RS-232 (Estándar recomendado 232). El componente de la capa de enlace de datos define el protocolo que establece la conexión entre el dispositivo DTE, que puede ser un enrutador y el dispositivo DCE, que puede ser un switch.

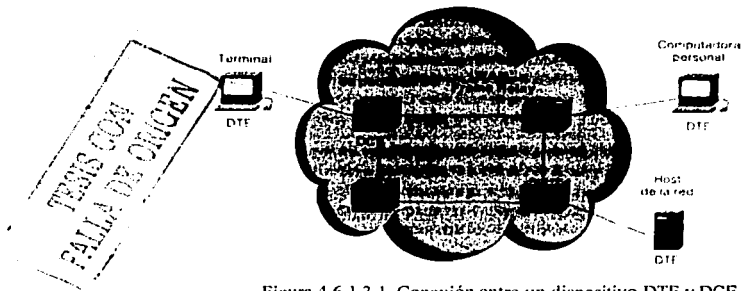


Figura 4.6.1.3.1. Conexión entre un dispositivo DTE y DCE.

#### 4.6.1.4 Circuitos Virtuales Frame Relay.

Frame Relay ofrece comunicación de la capa de enlaces de datos orientada a la conexión; esto significa que hay una comunicación definida entre cada par de dispositivos y que estas conexiones están asociadas con el identificador (DLCI) de conexión. Este servicio se implementa por medio de una *circuito virtual Frame Relay*, que es una conexión lógica creada entre dos DTE (Equipos Terminales de Datos) a través de una PSN (Red de Comunicación de Paquetes) de Frame Relay.

Los circuitos Virtuales ofrecen una trayectoria de comunicación bidireccional de un dispositivo DTE a otro y se identifica de manera única por medio del DLCI (Identificador de Conexiones de Enlace de Datos). Se puede multiplexar una gran cantidad de circuitos virtuales en un solo circuito físico para transmitirlos a través de la red. Con frecuencia esta característica permite conectar múltiples dispositivos DTE con menos equipo y una red compleja.

Un circuito virtual puede pasar por cualquier cantidad de dispositivos intermedios DCE (Switches) ubicados en la red Frame Relay PSN.

Los circuitos virtuales Frame Relay caen dentro de dos categorías: SVCs (Circuitos Virtuales Conmutados) y PVCs (Circuitos Virtuales Permanentes).

#### 4.6.1.5 Circuitos Virtuales Conmutados (SVC o *switched virtual circuit*).

Los SVCs son conexiones temporales que se utilizan en situaciones donde se requiere solamente de una transferencia de datos esporádica entre los dispositivos DTE a través de la red Frame Relay. La operación de una sesión de comunicación a través de un SVC consta de cuatro estados:

- *Establecimiento de la llamada*- Se establece el circuito virtual entre dos dispositivos DTE Frame Relay.
- *Transferencia de datos*- Los datos se transmiten entre los dispositivos DTE a través del circuito virtual.
- *Ocioso*- La conexión entre los dispositivos DTE aún está activa, sin embargo no hay transferencia de datos. Si un SVC permanece en estado ocioso por un periodo definido de tiempo, la llamada puede darse por terminada.
- *Terminación de la llamada*- Se da por terminado el circuito virtual entre los dispositivos DTE.

Una vez finalizado un circuito virtual los dispositivos DTE deben establecer un nuevo SVC si hay más datos que intercambiar. Se espera que los SVC se establezcan, conserven y finalicen utilizando los mismos protocolos de finalización que se usan en ISDN. Sin embargo, pocos fabricantes de equipo DCE Frame Relay soportan SVCs. Por lo tanto, su utilización real es mínima en las redes Frame Relay actuales.

#### 4.6.1.6 Circuitos Virtuales Permanentes (PVC o *private virtual circuit*).

Los PVCs son conexiones establecidas en forma permanente, que se utilizan en transferencia de datos frecuentes y constantes entre dispositivos DTE a través de la red Frame Relay. La comunicación a través de un PVC no requiere los estados de establecimiento de llamada y finalización que se utilizan con los SVCs. Los PVCs siempre operan en alguno de los estados siguientes:

- *Transferencia de datos*- Los datos se transmiten entre los dispositivos DTE a través del circuito virtual.
- *Ocioso*- Ocurre cuando la conexión entre los dispositivos DTE está activa, pero no hay transferencia de datos. A diferencia de los SVCs los PVCs no se darán por finalizados en ninguna circunstancia ya que se encuentran en estado ocioso.

Los dispositivos DTE pueden comenzar la transferencia de datos en cuanto estén listos, pues el circuito está establecido de manera permanente.

#### 4.6.1.7 Identificador de Conexión del Enlace de Datos (DLCI)(Data Link Connection Identifier).

Los circuitos virtuales de Frame Relay se identifican a través de los DLCI's (Identificadores de Conexión del Enlace de Datos). Normalmente los valores de DLCI son asignados por el proveedor de los servicios de Frame Relay (en su caso, la compañía telefónica). Los DLCI's Frame Relay tiene un significado local, lo que significa que los valores en sí mismo no son únicos en la WAN Frame Relay; por ejemplo, dos dispositivos DTE conectados a través de un circuito virtual, pueden usar un valor diferente de DLCI para hacer referencia a la misma conexión. La figura 4.6.1.7.1 muestra cómo se puede asignar a un solo circuito virtual un valor DLCI diferente en cada extremo de la conexión.

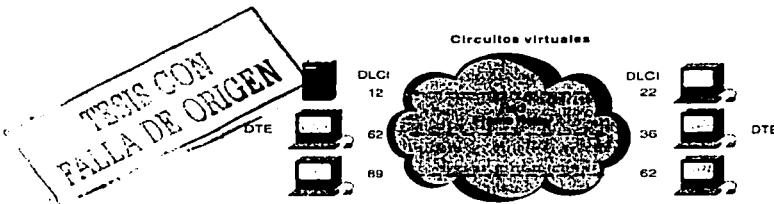


Figura 4.6.1.7.1 Asignación del DLCI a un solo circuito virtual

#### 4.6.1.8 Mecanismos de control de saturación.

Frame Relay reduce el gasto indirecto de la red, al implementar mecanismos simples de notificación de la saturación, mas que un control de flujo explícito por cada circuito virtual. En general Frame Relay se implementa sobre medios de transmisión de red confiables para no sacrificar la integridad de los datos, ya que el control de flujo se puede realizar por medio de los protocolos de las capas superiores. La tecnología Frame Relay implementa dos mecanismos de notificación de saturación:

- FECN (Notificación de la Saturación Explícita Hacia Adelante)
- BECN (Notificación de la Saturación explícita Hacia atrás)

Tanto FECN como BECN son controlados por un solo bit incluido en el encabezado de la trama Frame Relay. Este también contiene un bit DE (Elegibilidad para descarte), que se utiliza para identificar el tráfico menos importante que se puede eliminar durante periodos de saturación.

El bit FECN es parte del campo direcciones en el encabezado de la trama Frame Relay. El mecanismo FECN inicia en el momento en que un dispositivo DTE envía tramas Frame Relay a la red. Si la red está saturada, los dispositivos DCE (switches) fijan el valor de los bits FECN de las tramas en 1. Cuando las tramas llegan al dispositivo DTE de destino, el campo de direcciones (con el bit FECN en 1) indica que la trama se saturó en su trayectoria del origen al destino. El dispositivo DTE puede enviar esta información a un protocolo de las capas superiores para su procesamiento. Dependiendo de la implementación, el control de flujo puede iniciarse o bien la indicación se puede ignorar.

El bit BECN es parte del campo Direcciones del encabezado de la trama Frame Relay. Los dispositivos del DCE fijan el valor del bit BECN en 1 en las que viajan en sentido opuesto a las tramas con bit FECN igual a 1. Esto permite al dispositivo DTE receptor saber que una trayectoria específica en la red está saturada.

Posteriormente el dispositivo DTE envía información a un protocolo de las capas superiores para su procesamiento. Dependiendo de la implementación, el control de flujo puede iniciarse o bien se puede ignorar la indicación.

#### 4.6.1.9 BIT DE (Descart Elegibility).

El bit DE (Elegibilidad para Descarte) se utiliza para indicar que una trama tiene una importancia menor a otras. El bit DE es parte del campo Direcciones en el Encabezado de la trama Frame Relay.

Los dispositivos DTE pueden fijar el valor del bit DE de una trama en 1 para indicar que esta tiene una importancia menor respecto a las demás tramas. Al saturarse la red los dispositivos DCE descartaran las tramas con el bit DE fijado en 1 antes de descartar aquellas que no la tienen. Por lo anterior disminuye la probabilidad de que los dispositivos DCE de frame Relay eliminen datos críticos durante el blindaje de saturación lo que significa darle preferencia a este tipo de tramas.

#### 4.6.1.10 Verificación de errores en frame relay.

Frame Relay utiliza un mecanismo para la verificación de errores conocido como CRC (Verificación de Redundancia cíclica). El CRC compara dos valores calculados para determinar si se ha presentado errores durante la transmisión del origen al destino. Frame Relay disminuye el gasto indirecto al implementarse la verificación de errores mas que su corrección. Frame Relay por lo general se implementa en medios confiables de transmisión de red, por lo que la integridad de los datos no se sacrifica, si la corrección de un error se deja a los protocolos de las capas superiores que operan en la parte más alta de Frame Relay.

#### 4.6.1.11 Interfase LMI.

LMI (Interfase de la Administración Local) es un conjunto de avances en la especificación básica de Frame Relay. LMI fue desarrollada en 1990 por Cisco Systems, StrataCom, Northern Telecom y Digital Equipment Corporation. Presenta varias características (llamadas extensiones) para la administración de interredes complejas. Entre las extensiones LMI mas importantes de Frame Relay están el direccionamiento Global, los mensajes de estatus de los circuitos virtuales y la multidifusión.

La extensión de direccionamiento global LMI otorga los valores del DLCI (Identificador de la Conexión de Enlace de Datos) Frame Relay un significado global mas que local. Los valores DLCI se convierten en direcciones DTE únicas al enrutador WAN Frame Relay. La extensión global de direccionamiento agrega funcionalidad y buena administración a las interredes Frame Relay; por ejemplo, las interfases de red individuales y los nodos terminales conectados a ellos se pueden identificar por medio de técnicas estándar de



descubrimiento y resolución de direcciones. Además, para los routers ubicados en su periferia, toda la red Frame Relay aparece como una típica LAN.

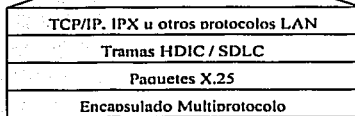
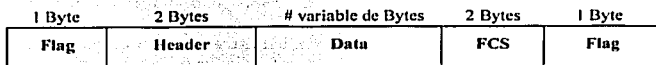
Los mensajes de status de los circuitos virtuales LMI permiten la comunicación y sincronización entre los dispositivos DTE y DCE Frame Relay. Estos mensajes se utilizan para reportar, de manera periódica, el status de los PVCs; así se previene el envío de datos a PVC's inexistentes.

La extensión de LMI para multidifusión permite que se asignen grupos de multidifusión. Con la multidifusión se ahorra ancho de banda, ya que permite que los mensajes sobre la resolución de direcciones y de actualizaciones de enrutamiento s

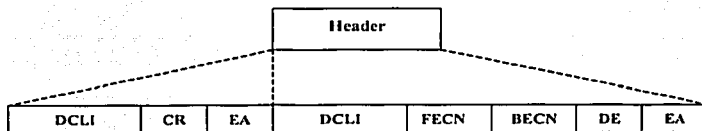
**TRIS CON  
FALLA DE ORIGEN**

#### 4.6.1.12 Formato de la trama de Frame Relay.

Formato estándar de Frame Relay



Descripción del Campo Header



DLCI=Data Connection Identifier  
 CR=Command Response Bit  
 FECN=Forward Explicit Congestion Notification  
 BECN=Backward Explicit Congestion Notification  
 EA=Adress Extension Bit indicate extended adress

ean enviados solamente a grupos específicos de enrutadores. La extensión también permite reportes sobre el status de los grupos de multidifusión de los mensajes de actualización.

<b>Flags</b>	Delimitan el comienzo y la terminación de la trama. El valor de este campo es siempre el mismo y se representa con el número hexadecimal 7E o el número binario 01111110.
<b>Header</b>	Contiene la información siguiente

	<ul style="list-style-type: none"> <li>• <b>DLCI:</b> El DLCI es la esencia del encabezado de Frame Relay. Este valor representa la conexión virtual entre el dispositivo DTE y el switch. Cada conexión virtual que se multiplexa en el canal físico será representada por un DLCI único. Los valores del DLCI tienen significado local solamente, lo que indica que son únicos para el canal físico en que residen; por lo tanto, los dispositivos que se encuentran en los extremos opuestos de una conexión pueden utilizar diferentes valores DLCI para hacer referencia a la misma conexión virtual.</li> <li>• <b>EA (dirección extendida):</b> La EA se utiliza para indicar si el byte cuyo valor EA es 1, es el último campo de direccionamiento. Si el valor es 1, entonces se determina que este byte sea el último octeto DLCI. Aunque todas las implementaciones actuales de Frame Relay utilizan un DLCI de dos octetos, esta característica permitirá que en el futuro se utilicen DLCIs más largos. El octavo bit de cada byte del campo de direcciones de utiliza para indicar el EA.</li> <li>• <b>C/R:</b> El C/R es el bit que sigue después del byte DLCI más significativo en el campo de direcciones. El bit C/R no está definido hasta el momento.</li> <li>• <b>Control de saturación:</b> Este campo consta de 3 bits que controlan los mecanismos de notificación de la saturación en Frame Relay. Éstos son los bits FECN, BECN y DE, que son los últimos bits en el campo de direcciones.</li> <li>• <b>FECN (notificación de la Saturación Explícita Hacia Adelante):</b> Es un campo de un solo bit que puede fijarse con el valor de 1 por medio de un interruptor para indicar a un dispositivo DTE terminal, como un enrutador, que ha habido saturación en la dirección de la trama del origen al destino. La ventaja principal de usar los campos FECN y BECN es la habilidad que tienen los protocolos de las capas superiores de reaccionar de manera inteligente ante estos indicadores de saturación.</li> <li>• <b>BECN (Notificación de Saturación Explícita Hacia Atrás):</b> Es un campo de un solo bit que, al ser establecido en 1 el valor por un switch, indica que ha habido saturación en la red en la dirección opuesta a la de la transmisión de la trama desde el origen al destino.</li> <li>• <b>DE (Eligibilidad para Descartes):</b> Este bit es fijado por el dispositivo DTE, un enrutador por ejemplo, para indicar que la trama marcada es de menor importancia en relación con otras tramas que se marcan como "elegible para descartes" deben ser descartadas antes de cualquier otra. Lo anterior representa un mecanismo justo de establecimiento de prioridad en las redes Frame Relay.</li> </ul>
<b>Datos</b>	Los datos contienen información encapsulada de las capas superiores. Cada trama en este campo de longitud variable incluye un campo de datos de usuario o carga útil que varía en longitud y podrá tener hasta 16,000 bytes. Este campo sirve para transportar el PDU (Paquete de Protocolo de las Capas Superiores) a través de una red Frame Relay.
<b>FSC</b>	Asegura la integridad de los datos transmitidos. Este valor calculado por el dispositivo de origen y verificado por el receptor para asegurar la integridad de la transmisión.

#### 4.6.1.13 Formato de la trama LMI

Las tramas Frame Relay que siguen las especificaciones LMI contienen los campos que se muestran en la figura:

Flag	Encabezado	Indicador de tramas no numeradas	Discriminador de Protocolos	Referencia a llamada	Tipo de Mensaje	Elementos de información	FCS	Flag
------	------------	----------------------------------	-----------------------------	----------------------	-----------------	--------------------------	-----	------

<b>Flag</b>	Delimita el comienzo y el final de la trama.
-------------	--

<b>Encabezado LMI DLCI</b>	Identifica la trama como una trama LMI en vez de una trama básica Frame Relay. El valor DLCI específico del LMI definido por la especificación del consorcio LMI es DLCI = 1023.
<b>Indicador de la información no numerada</b>	Fija el bit sondeo/final en cero.
<b>Discriminador de protocolos</b>	Siempre contiene un valor que indica que es una trama LMI.
<b>Referencia de llamada</b>	Siempre contiene ceros. En la actualidad este campo no se usa ni tiene ningún propósito.
<b>Tipo de mensaje</b>	Etiqueta la trama con uno de los siguientes tipos de mensaje: <ul style="list-style-type: none"> <li>• Mensaje de solicitud de status: Permite que un dispositivo de usuario solicite el status de la red</li> <li>• Mensaje de status: Responde a los mensajes de solicitud de status. Los mensajes de status incluyen mensajes de sobrevivencia y de status del PVC,</li> </ul>
<b>Elementos de información</b>	Contiene una cantidad variable de IEs (Elementos Individuales de Información). Los IEs constan de los campos siguientes: <ul style="list-style-type: none"> <li>• Identificador IE: Identifica de manera única el IE</li> <li>• Longitud del IE: Indica la longitud del IE</li> <li>• Datos: Consta de uno o más bytes que contienen datos encapsulados de las capas superiores</li> </ul>
<b>FCS</b>	Asegura la integridad de los datos transmitidos.

#### 4.6.2 ATM.

##### 4.6.2.1 Definición.

ATM se basa en el concepto de Conmutación Rápida de Paquetes (Fast Packet Switching) en el que se supone una fiabilidad muy alta a la tecnología de transmisión digital, típicamente sobre fibra óptica, y por lo tanto la no necesidad de recuperación de errores en cada nodo. Ya que no hay recuperación de errores, no son necesarios los contadores de número de secuencia de las redes de datos tradicionales, tampoco se utilizan direcciones de red ya que ATM es una tecnología orientada a conexión, en su lugar se utiliza el concepto de Identificador de Circuito o Conexión Virtual (VCI).

El tráfico con tasa de bit o velocidad binaria constante (CBR), por ejemplo voz PCM o vídeo no comprimido, tradicionalmente es transmitido y conmutado por redes de conmutación de circuitos o Multiplexores por División en el Tiempo (TDM), que utilizan el Modo de Transmisión Síncrono (STM). En STM, los multiplexores por división en el tiempo dividen el ancho de banda que conecta dos nodos, en contenedores temporales de tamaño pequeño y fijo o ranuras de tiempo ("Time Slots"). Cuando se establece una conexión, esta tiene estadísticamente asignado un "slot" (o varios). El ancho de banda asociado con este "slot" está reservado para la conexión haya o no transmisión de información útil. Una pequeña cantidad de ancho de banda para control, se utiliza para la comunicación entre los conmutadores, de forma que estos conocen los "slots" que tiene asignados la conexión. Esto se conoce como direccionamiento implícito. El conmutador

receptor sabe a que canales corresponden los "slots" y por lo tanto no se requiere ningún direccionamiento adicional. Este procedimiento garantiza la permanente asignación de un ancho de banda durante el tiempo que dura la llamada, así como un tiempo de retardo pequeño y constante.

En contraste, los datos son normalmente transmitidos en forma de tramas o paquetes de longitud variable, lo que se adecua bien a la naturaleza de ráfagas de este tipo de información. Sin embargo, este mecanismo de transporte tiene retardos impredecibles, la latencia tiende a ser alta y en consecuencia la conmutación de paquetes no es adecuada para tráfico con tasa de bit constante como la voz. Tampoco la conmutación de circuitos se adecua para la transmisión de datos, ya que si se asigna un ancho de banda durante todo el tiempo para un tráfico en ráfagas, se derrocha mucho ancho de banda cuando este no se utiliza.

ATM ha sido definido para soportar de forma flexible, la conmutación y transmisión de tráfico multimedia comprendiendo datos, voz, imágenes y vídeo. En este sentido, ATM soporta servicios en modo circuito, similar a la conmutación de circuitos, y servicios en modo paquete, para datos (figura 4.6.2.1.1).

**tráfico con FALLA DE ORIGEN**

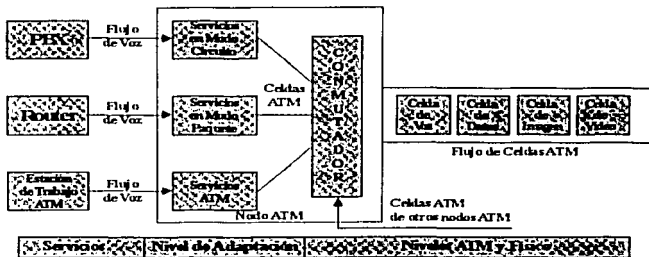
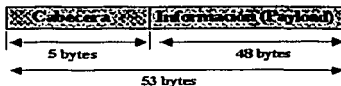


Figura 4.6.2.1.1. Funcionamiento de un Nodo ATM

Sin embargo, a diferencia de la conmutación de circuitos, ATM no reserva "slots" para la conexión. En su lugar, una conexión obtiene "slots" o celdas, solo cuando está transmitiendo información. Cuando una conexión está en silencio no utiliza "slots" o celdas, estando estas disponibles para otras conexiones. Con esta idea en mente, se decidió que la unidad de conmutación y transmisión fuese de tamaño fijo y longitud pequeña. Esta unidad es conocida como Celda, y tiene una longitud de 53 bytes divididos en 5 de cabecera y 48 de información o carga útil. Esta celda es quien viene a sustituir al "Time Slot" de una Red TDM (ver figura 4.6.2.1.2).



Longitud fija: 53 bytes  
 Tamaño pequeño  
 Figura 4.6.2.1.2. Celda ATM

Las celdas pequeñas y de longitud constante son ventajosas para tráfico con tasa de bit constante (Voz, Video) y son muy útiles en general ya que permiten un tiempo de latencia muy bajo, constante y predecible, así como una conmutación por hardware a velocidades muy elevadas. También, en el caso de pérdida de celdas por congestión o corrupción, la pérdida no es muy grande siendo en muchos casos remediable o recuperable. De hecho, el tráfico de Voz y Vídeo, no es muy sensible a pequeñas pérdidas de información,

pero si es muy sensible a retardos variables, sucediéndole lo contrario al tráfico de datos. En una red ATM, donde las celdas no están reservadas sino asignadas bajo demanda, el conmutador receptor no puede determinar por adelantado a que canal corresponde cada celda. La Celda ATM a diferencia del Time Slot en TDM, debe transportar la identificación de la conexión a la que pertenece, de esta forma no existirán celdas vacías ya que serán utilizadas por conexiones pendientes. Esta es una diferencia fundamental del ATM frente al TDM. La cabecera presente en cada celda, consume aproximadamente un 9.5% del ancho de banda, siendo este el precio que hay que pagar por la capacidad para disponer de ancho de banda bajo demanda, en lugar de tenerlo permanentemente reservado y eventualmente desperdiciado. La adopción de una cabecera de 5 bytes ha sido posible, porque no se realiza recuperación de errores en los nodos intermedios, tampoco se emplean direcciones válidas a nivel de toda la red, tales como la dirección MAC en Ethernet o IP en redes tipo TCP/IP (ver figura 4.6.2.1.3).

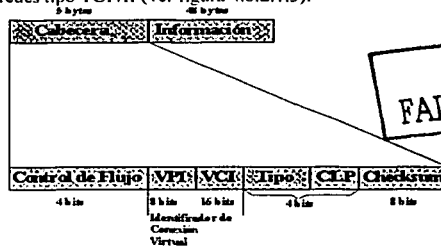


Figura 4.6.2.1.3. Cabecera de la Celda ATM

Al igual que en las redes de conmutación de paquetes (X.25 y Frame Relay), la tecnología ATM está Orientada a Conexión. Esto significa que antes de que el usuario pueda enviar celdas a la red, es necesario realizar una llamada y que esta sea aceptada para establecer una Conexión Virtual a través de la red. Durante la fase de llamada un Identificador de Conexión Virtual (VCI) es asignado a la llamada en cada nodo de intercambio a lo largo de la ruta (ver figura 4.6.2.1.4).



Figura 4.6.2.1.4. Identificador de conexión virtual (VCI)

El identificador asignado, sin embargo, solo tiene significado a nivel del enlace local, y cambia de un enlace al siguiente según las celdas pertenecientes a una conexión pasan a través de cada conmutador ATM. Esto significa, que la información de enrutamiento (routing) transportada por cada cabecera puede ser relativamente pequeña.

Asociado con cada enlace o puerto entrante del conmutador ATM, hay una tabla de enrutamiento que contiene el enlace o puerto de salida y el nuevo VCI que va a ser utilizado en correspondencia a cada VCI entrante (ver figura 4.6.2.1.5).

**TEJAS CON FALLA DE ORIGEN**

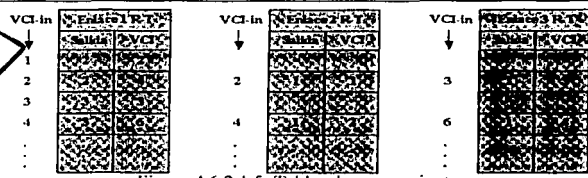


Figura 4.6.2.1.5. Tablas de enrutamiento

De este modo el enrutamiento de celdas en ambas direcciones a lo largo de la ruta es extremadamente rápido, ya que consiste en una simple operación de consulta en una tabla. Como resultado, las celdas procedentes de cada enlace pueden ser conmutadas independientemente a velocidades muy altas. Esto permite el uso de arquitecturas de conmutación paralelas y circuitos de alta velocidad hasta gigabits, cada uno operando a su máxima capacidad. Celdas procedentes de diferentes fuentes son multiplexadas juntas de forma estadística a efectos de conmutación y transmisión.

Un conmutador ATM podría describirse como una caja que mantiene en su interior una gran cantidad de Ancho de Banda, siendo este recurso cedido o recuperado dinámicamente según el aumento o disminución de las necesidades. En este sentido, se dice que ATM proporciona Ancho de Banda bajo demanda.

**4.6.2.2 Modelo de Referencia ATM**

El modelo de referencia propuesto por el CCITT está constituido por tres niveles: Nivel Físico, Nivel ATM y Nivel de Adaptación ATM (AAL) (ver figura 4.6.2.2.1).

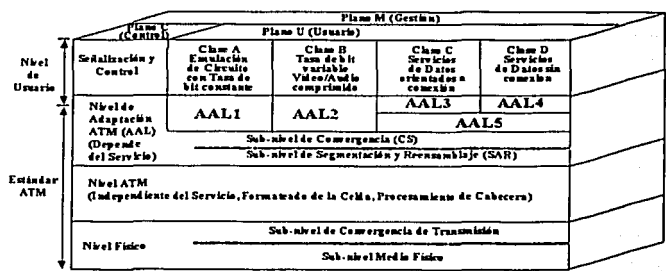


Figura 4.6.2.2.1 Modelo de Referencia ATM

Las funciones han sido divididas en tres grupos conocidos como planos: El plano C de control y señalización, el plano U de usuario y el plano M de gestión. Los protocolos del plano C se encargan de la señalización, es decir, del establecimiento, mantenimiento y cancelación de conexiones virtuales. Los protocolos del plano U dependen de la aplicación y en general operan extremo a extremo (usuario a usuario). Los protocolos del plano M se encargan de la Operación, Administración y Mantenimiento (OAM). Los protocolos de los tres planos hacen uso de los servicios ofrecidos por los tres niveles ATM.

**4.6.2.2.1 Nivel Físico.**

Define las interfases físicas, los protocolos de trama y codificación para la red ATM. Hay diferentes opciones de conexiones físicas. La especificación del ATM Forum con relación a la Interfase Usuario Red (ATM UNI) actualmente define SONET/SDH STS-3c (155.52 Mbps), DS3(44.736 Mbps), E3(34.368 Mbps), posiblemente DS1/E1, así como 100 Mbps con codificación 4B/5B para fibra local (derivado del estándar FDDI a.k.a. TAXI) y 155 Mbps con codificación 8B/10B sobre fibra óptica multimodo (basado en Fibre Channel). Existen varias propuestas para el uso de Par Trenzado apantallado (STP) o sin apantallado (UTP), enfrentándose todas ellas al problema común de transmitir 100+ Mbps sobre la extensa base instalada de UTP (principalmente tipo 3) sin violar los límites de interferencia del FCC. El ATM Forum ha aprobado las especificaciones para UTP Categoría 5 con codificación SONET STS-3c a 155.52 Mbps, así como UTP Categoría 3 con codificación SONET STS-1 a 51.84 Mbps. IBM propone UTP Categoría 3 con codificación 4B/5B a 25.6 Mbps.

Cada conexión física al conmutador ATM es un enlace dedicado y todos los enlaces pueden estar simultáneamente activos. Los conmutadores ATM están diseñados para permitir a todos los puertos comunicarse transparentemente e independiente de la velocidad física. Esto permite que la conexión física esté acoplada con los requerimientos de ancho de banda del dispositivo conectado. La conversión de velocidad es una característica inherente de ATM, tampoco tiene restricciones topológicas de las redes clásicas tales como Token Ring o Ethernet.

El nivel físico (PHY), proporciona al nivel ATM con los medios para transportar celdas ya configuradas. Este nivel está dividido en dos subniveles: el subnivel de Convergencia de Transmisión (TC), y el subnivel dependiente del Medio Físico (PM). La selección del medio físico determina la operación de ambos subniveles. El subnivel PM para cada medio, define cosas tales como formas de onda, ordenación de los bits, codificación en línea, recuperación del reloj, sincronización, etc. Además, para tráfico con temporización relacionada, proporciona información de temporización al nivel de Adaptación ATM (AAL).

Pero el subnivel TC es la clave para que la celda ATM, viaje libremente sobre una amplia variedad de medios. El subnivel TC empaqueta las celdas ATM salientes en la estructura de trama del medio de transmisión, rellenando con celdas nulas según se necesite. A la recepción, el subnivel TC determina los contornos de las celdas, extrayéndolas del flujo de bits, descartando celdas nulas o erróneas y finalmente entregándolas al nivel ATM.

#### 4.6.2.2.2 Nivel ATM.

Este es el nivel de conmutación y transmisión de ATM. Define la estructura de la cabecera de la celda, y como las celdas fluyen sobre las conexiones lógicas en la red ATM. Realiza las funciones de multiplexación estadística de celdas procedentes de diferentes conexiones, y su enrutamiento sobre las conexiones virtuales. Las conexiones lógicas en el nivel ATM, están basadas en el concepto de Camino Virtual (Virtual Path) y Canal Virtual (Virtual Channel). Una Conexión de Camino Virtual (VPC) es una colección de Conexiones de Canal Virtual (VCC) tributarios que son transportados a lo largo del mismo camino o ruta. Un conmutador de tránsito podría reaccionar únicamente a la información de camino (VPC), mientras que los conmutadores terminales reaccionarían a la información de fan-out (VCC), pudiéndose mapear diferentes sesiones contra VCI's sobre la misma conexión VPC.

Cada VPC o VCC puede estar establecido permanentemente, con lo que tendremos una Conexión Virtual Permanente (PVC), o establecido dinámicamente bajo demanda disponiéndose entonces, de una Conexión Virtual Conmutada (SVC). Funciones de control y señalización asociadas con el plano C, y por lo tanto fuera del modelo de referencia ATM, permiten al usuario establecer y terminar dinámicamente VPC's y VCC's (ver figura 4.6.2.2.2.1).

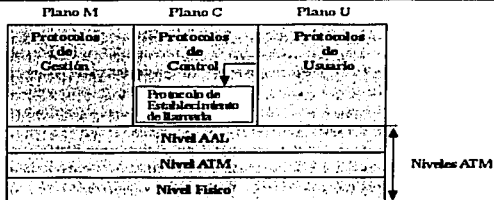


Figura 4.6.2.2.2.1. Protocolos externos a ATM

Dentro de una red ATM, el camino seguido por los mensajes de señalización es una conexión virtual específica conocida como Conexión de Canal Virtual para Señalización (SVCC). Un descriptor de tráfico, o contrato usuario-red, define los parámetros y reglas de cada VPC y VCC. Están especificados descriptores de tráfico definiendo pico de tráfico (PCR), longitud máxima de ráfagas (MBS), tasa de bit media (SCR), variación del retardo (CDVT). El protocolo de control de la conexión negocia la clase de servicio específica y las características del ancho de banda de cada circuito virtual durante el establecimiento de la llamada. La red propaga esa petición internamente hasta su destino y verifica si los requerimientos exigidos se van a poder cumplir. En caso afirmativo, la red acepta el circuito y a partir de ese momento, garantiza que el tráfico se va a tratar acorde a las condiciones negociadas en el establecimiento. Esto permite que cada circuito virtual sea cortado a medida para su uso específico, por ejemplo vídeo o paquetes de datos, siendo la calidad del servicio (QoS) una característica inherente de ATM.

Hay dos formatos diferentes para la encabezado o cabecera de las celdas (ver figura 4.6.2.2.2.2).

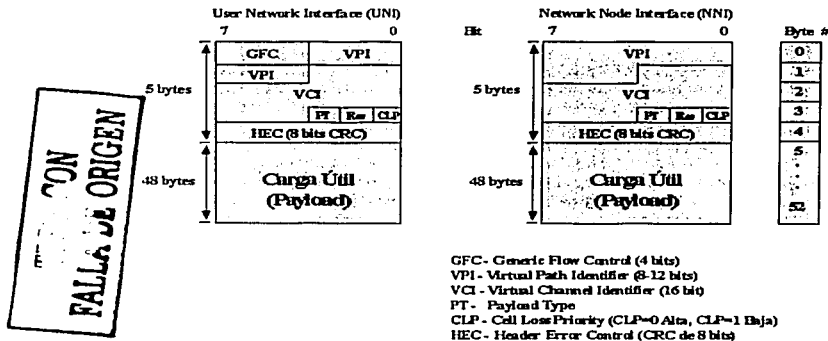


Figura 4.6.2.2.2.2 Formatos UNI (User to Network Interface) y NNI( Network to Network Interface)

El primero proporciona la conexión a la Red ATM desde un equipo terminal ATM o bien desde un sistema intermedio, IS, tal como un Hub un puente o un encaminador que a su vez controla equipos de usuario final.



El segundo define la interfaz entre dos nodos ATM; cuando la NNI conecta nodos pertenecientes a distintas redes se denomina NNI-ICI, es decir, NNI-ICI, es decir NNI-Inter Carrier Interface.

El campo Control de Flujo Genérico (GFC) tiene significado únicamente en este enlace y se incluye para asignar prioridades a las diferentes celdas, dependiendo del tipo de información que transportan, y que estas sean colocadas en diferentes colas de salida según su prioridad. No está presente dentro de la red, y en su lugar se amplía el campo VPI.

El campo Tipo de Carga útil (PT) se utiliza para permitir que las celdas de los planos C y M, se distingan de las celdas conteniendo información de Usuario, y también para informar de la existencia de congestión. El protocolo AAL5 utiliza un bit del campo PT para indicar el fin del mensaje (EOM) de una trama AAL5 (PT=0x1). El bit CLP permite que las celdas tengan una de dos prioridades: alta (CLP=0) y baja (CLP=1). Debido a que un conmutador ATM opera por multiplexación estadística de sus entradas, es posible que múltiples entradas compitan por una misma salida, dando lugar a que un buffer temporal se desborde en un enlace de salida de un nodo ATM. El bit CLP se utiliza para marcar aquellas celdas que en caso de congestión se puedan descartar primero. El campo HEC es un CRC de 8 bits para detección de errores en la cabecera (solo), especialmente si el direccionamiento es correcto. Si falla, la celda es descartada. Si es correcto, se puede proceder inmediatamente a la conmutación. Celdas vacías también son descartadas y se caracterizan por que su VPI/VCI es cero.

#### 4.6.2.2.3 Nivel de Adaptación ATM (AAL)

Como se ha indicado, ATM ha sido definido para proporcionar un soporte de conmutación y transmisión flexible para tráfico multimedia. En consecuencia, es esencial que ATM soporte un rango de tipos de servicios alternativos. Mas aun, excepto para aquellas aplicaciones que generan directamente celdas, el uso de la conmutación y transmisión de celdas tiene que ser totalmente transparente al equipo del usuario. El nivel de Adaptación ATM, como su nombre indica, realiza las funciones de adaptación (convergencia) entre las clases de servicio proporcionadas al usuario, por ejemplo transportar tramas de datos entre dos LAN's, y el servicio basado en celdas proporcionado por ATM.

Cuando una trama o flujo de bits, cualquiera que sea su origen (voz, datos, imagen o vídeo), entra en una red ATM, el nivel de Adaptación la segmenta en celdas. El proceso comienza inmediatamente cuando la primera parte de la trama entra en el conmutador de acceso a la red ATM; no hay que esperar hasta que la trama entera haya llegado (figura 4.6.2.2.3.1).

CON  
 FALLA DE ORIGEN

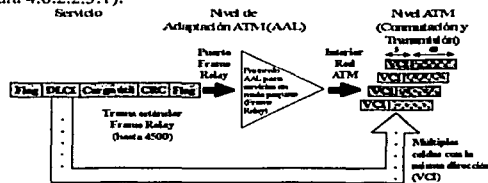


Figura 4.6.2.2.3.1 Servicios en modo paquete

Las celdas generadas son enviadas a través de la red ATM a alta velocidad, por ejemplo a 622 Mbps. Durante la totalidad del proceso, hay únicamente un punto donde la trama completa podría estar almacenada: en el punto de salida de la red, sin embargo bastará que haya un número suficiente de celdas en el punto de salida para comenzar la entrega al usuario.

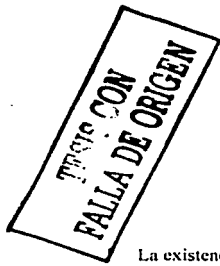
En los conmutadores intermedios, todas las celdas son despachadas tan rápidamente como llegan. De hecho, en el momento que la trama ha entrado totalmente en el conmutador de acceso a la red, la mayor parte de la trama estará ya en el puerto de destino, próxima a salir o saliendo de la red ATM. Esta tecnología evita el retardo de señalización causado por otras técnicas, que emplean la aproximación de almacenamiento de la trama y su posterior envío. También la utilización de celdas de tamaño pequeño y fijo, permite el intercalado

y priorización de celdas en los buffers de salida de los conmutadores ATM, reduciéndose la sensibilidad a la congestión.

AAL soporta cuatro tipos de servicios: Clases A, B, C y D. Hay cuatro tipos de AAL: AAL1 y AAL2 soportan las clases A y B respectivamente, mientras que las clases C y D están indistintamente soportadas por AAL3/4 ó AAL5. El protocolo AAL5 es una versión más sencilla y eficiente de la AAL 3/4, soportando las clases de servicio C y D para datos de alta velocidad. El nivel AAL realiza funciones de Segmentación y Reensamblado (SAR) para mapear la información de niveles superiores, al campo de Carga Util del la celda. Otras funciones de AAL son el control y recuperación de la temporización para las clases de servicio A y B, así como la detección y manejo de celdas perdidas o fuera de secuencia.

#### 4.6.2.2.4 Clases de Servicios.

Los servicios han sido clasificados de acuerdo con tres criterios:



Clase A	Clase B	Clase C	Clase D	Clase de Servicios
Si		No		
Constante	Variable			Tasa de bit
Orientado a conexión			Sin conexión	Modo

Figura 4.6.2.2.4.1. Servicios proporcionados por ATM

- La existencia de una temporización relacionada entre los usuarios origen y destino (por ejemplo voz).
- La tasa de bit, o velocidad binaria asociada con la transferencia (constante/CBR o variable/VBR).
- El modo de conexión (con conexión o sin conexión).

Los servicios en clase A y B están orientados a conexión y existe una temporización relacionada entre los usuarios origen y destino. La diferencia entre las dos clases, es que la clase A proporciona un servicio con tasa de bit constante, mientras que en la clase B la tasa de bit es variable. Un ejemplo de uso de la clase A, es la transferencia de un flujo constante de bits asociada con una llamada de voz, por ejemplo a 64Kbps (Similar a un canal B en ISDN). La clase A es también conocida, como Emulación de Circuito Conmutado.

Un ejemplo de uso de la clase B, es la transmisión de un flujo de bits variable asociado con vídeo comprimido. Aunque el vídeo produce tramas a velocidad constante, un codec de vídeo produce tramas conteniendo una cantidad variable de datos comprimidos.

Las clases C y D no tienen temporización relacionada entre el origen y el destino. Ambas proporcionan servicios en modo paquete, con velocidad binaria variable entre origen y destino. La clase C está orientada a conexión y la clase D es sin conexión.

Para realizar las funciones anteriores, el nivel AAL está dividido en dos subniveles:

-El Sub-nivel de Convergencia (CS), que realiza las funciones de convergencia entre el servicio ofrecido al usuario y el proporcionado por el nivel ATM.

-El Sub-nivel de Segmentación y Reensamblado (SAR), que realiza las funciones de ensamblado/segmentación de los datos de origen para colocarlos en el campo de información de la celda y la correspondiente función de desensamblado/reensamblado en el destino.

Asociada con cada clase de servicio está un tipo de Punto de Acceso al Servicio (SAP) y un protocolo asociado. Clase A tiene un SAP de tipo 1, clase B de tipo 2 y así sucesivamente (ver figura 4.6.2.2.4.2).

TESIS CON FALLA DE ORIGEN

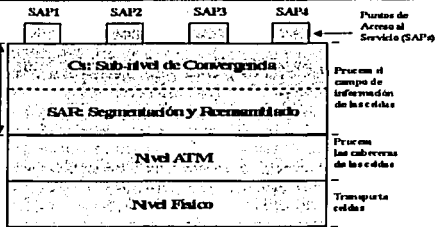


Figura 4.6.2.4.2 Puntos de Acceso al Servicio (SAPs)

Los cuatro tipos o clases de servicios utilizan los 48 bytes del campo de carga útil en cada celda de forma diferente, pudiendo opcionalmente contener un campo de hasta 4 bytes para adaptación ATM.

**Tipo 1: Velocidad Binaria Constante (CBR).**

En este tipo de servicio, el protocolo de AAL1 se esfuerza en mantener un flujo con tasa de bit constante entre los SAPs de origen y destino (entrega sincronizada). La velocidad binaria está en el rango de pocos kilobits por segundo, por ejemplo para voz comprimida, a decenas de megabits por segundo, por ejemplo en video no comprimido. Sin embargo, la velocidad binaria acordada debe ser mantenida, incluso con pérdidas ocasionales de celdas o variaciones en el tiempo de transferencia de las mismas. Este servicio se asemeja al proporcionado por el sistema telefónico existente, ya que garantiza un número fijo de celdas por unidad de tiempo para la aplicación.

El formato del campo de información de la celda, conocido como segmento, incluye un Número de Secuencia de 4 bits (SN) y un campo asociado de 4 bits utilizado para Proteger el Número de Secuencia (SNP) contra errores de un bit (ver figura 4.6.2.4.3).

**Tipo 1: Velocidad Binaria Constante (CBR)**

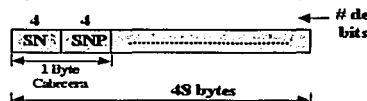


Figura 4.6.2.4.3. Formato del segmento CBR

De esta forma es posible detectar pérdidas de segmentos. Las pérdidas de celdas se superan de forma acordada; por ejemplo, insertando segmentos ficticios en el flujo entregado. Variaciones en el retardo de transferencia de celdas, son compensadas mediante un buffer en la parte destino; la salida de segmentos correspondiente a una llamada, únicamente se comienza después de que se hayan recibido un número predeterminado de segmentos, este número viene determinado por la velocidad binaria del usuario. Valores típicos son 2 segmentos a velocidades de kilobits y 100 segmentos a velocidades de megabits por segundo. Claramente este retardo se sumará al retardo de ensamblaje/desensamblaje ya identificado.

El uso de un buffer en destino también proporciona un modo sencillo de superar cualquier pequeña variación entre las velocidades binarias en origen y destino; por ejemplo si cada uno está basado en diferente reloj. Una solución mejor, es que la red proporcione los relojes de entrada y salida, normalmente extraídos de la codificación en línea del flujo de bits transmitido.

**Tipo 2: Velocidad Binaria Variable (VBR).**

En este tipo de servicio, aunque exista una temporización relacionada entre los SAPs fuente y el destino, la velocidad de transferencia real de información, puede variar durante la conexión. Como con el tipo 1, el segmento contiene un Número de Secuencia de 4 bits para la recuperación de celdas pérdidas (ver figura 4.6.2.4.4).

### Tipo 2: Velocidad Binaria Variable (VBR)

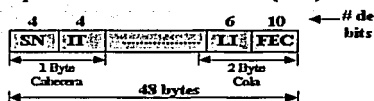


Figura 4.6.2.2.4.4 Formato del segmento VBR

El campo de Tipo de Información (IT) indica, o bien la posición relativa del segmento con relación al mensaje remitido, por ejemplo, una trama comprimida procedente de un video-codec, o si el segmento contiene información de temporización, o de otro tipo. Los tres tipos de segmento con relación a la información posicional son: comienzo de mensaje (BOM), continuación de mensaje (COM) y fin de mensaje (EOM). Debido al tamaño variable de las unidades de mensaje remitidas, un Indicador de Longitud (LI) en la cola del segmento indica el número de bytes útiles en el último segmento. Finalmente, el campo FEC habilita la detección y corrección de errores.

### Tipo 3: Datos Orientados a Conexión.

El protocolo AAL3/4 proporciona dos tipos de servicios para la transferencia de datos: uno Orientado a Conexión (CO) y otro Sin Conexión (CLS). La diferencia entre los dos es que con el primero, antes de que cualquier dato pueda ser transmitido, debe establecerse una Conexión Virtual.

El servicio orientado a conexión tiene dos modos operacionales: asegurado y no asegurado, cada uno soportando envíos de Unidades de Datos del Servicio (SDUs) o mensajes de usuario, de tamaño fijo o variable. El modo asegurado proporciona un servicio fiable que garantiza que todas las SDUs son entregadas sin errores y en la misma secuencia con que fueron remitidas. Este es un servicio similar al proporcionado por una red de conmutación de paquetes tipo X.25 y, para proporcionar este servicio, todos los segmentos generados por el sub-nivel CS están sujetos a procedimientos de control de flujo y recuperación de errores.

Para el modo no asegurado, los segmentos son transmitidos sobre la base del mejor intento; esto es, cualquier segmento corrompido es simplemente descartado y se deja a los niveles de protocolo de usuario superar esta eventualidad.

El Tipo de Segmento (ST) indica si es el primero (BOM), continuación (COM), último (EOM), o el único (SSM) de una SDU remitida.

### Tipo 3: Datos Orientado a Conexión

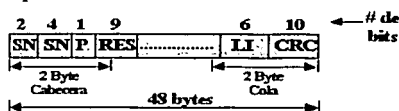


Figura 4.6.2.2.4.5 Formato del segmento con conexión

El Número de Secuencia (SN) se emplea para detectar segmentos perdidos o duplicados y también para control de flujo. Un único bit de Prioridad (P) permite que los segmentos tengan uno de dos niveles de prioridad. En la cola, el Indicador de Longitud (LI) indica el número de bytes útiles en el segmento y el CRC-10 está presente para la detección y eventual corrección de errores. Claramente LI solamente tiene significado en el último segmento de una SDU o si es el único segmento.

Los segmentos generados por el sub-nivel SAR del protocolo AAL3/4, son compatibles con la especificación IEEE 802.6 utilizada en el servicio SMDS.

El funcionamiento del protocolo del Sub-nivel de Convergencia (CS) se puede describir mejor, considerando el formato de los mensajes o Unidades de Datos del Protocolo (CS-PDU) que genera, en relación con la SDU remitida por el usuario, y el modo que esta es transportada por el sub-nivel SAR.

TESIS CON FALLA DE ORIGEN

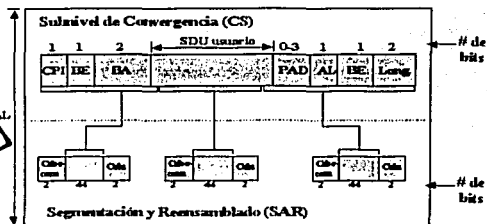


Figura 4.6.2.2.4.6. Protocolos AAL

Los campos de cabecera y cola añadidos por el protocolo CS en origen a la SDU remitida, se utilizan para habilitar al protocolo CS receptor la detección de SDUs perdidas o malformadas. El Identificador de Protocolo CS (CP1), se utiliza para identificar el tipo de protocolo CS que está siendo utilizado. El identificador comienzo-fin (BE) es un número de secuencia módulo 256 y se repite en cola para añadir capacidad de reacción. Se utiliza para asegurarse que las SDUs son entregadas en la misma secuencia en la que se remitieron. El campo de Asignación de Buffer (BA) se inserta en la cabecera para ayudar al protocolo CS receptor, a reservar una cantidad de memoria suficiente (buffer) para contener una SDU completa. En la cola, el campo de relleno (PAD) se utiliza para hacer que el número de bytes de la unidad de datos del protocolo CS, sea un múltiplo de 4 bytes. De forma similar, el byte de ALineamiento (AL) es un byte de relleno para hacer que la cola tenga 4 bytes. El campo de longitud (Length) indica la longitud total de la unidad de datos del protocolo completa y entonces ayuda al receptor a detectar cualquier SDU malformada.

**Tipo 4: Datos sin Conexión.**

El servicio de datos sin conexión es probablemente el primero que va a ser soportado. Está pensado, por ejemplo, para la interconexión de LANs a alta velocidad. A diferencia del tipo 3 no hay señalización de llamada ni terminación, en su lugar conexiones permanentes o semi-permanentes están siempre establecidas entre cada par de SAPs origen y destino. Aparte de esto, los dos servicios utilizan los mismos formatos en el Subnivel de Convergencia CS y segmento.

**Tipo 4: Datos sin Conexión**

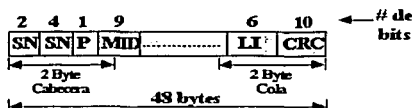


Figura 4.6.2.2.4.7. Formato del segmento sin conexión

Sin embargo, con los servicios sin conexión, el campo RES (reservado) está sustituido por el Identificador del Mensaje (MID). Normalmente celdas relacionadas con diferentes tramas estarán en tránsito en cualquier instante, el campo MID se utiliza para habilitar al subnivel SAR de destino relacionar cada celda recibida a su SDU específica. La utilización del MID permite la multiplexación de múltiples sesiones en una misma conexión virtual VPI/VC1.

**4.6.2.2.5 Servicios sin conexión ATM.**

---

Usualmente esta información será introducida por el gestor de la red y para minimizar la sobrecarga se deben utilizar varios de estos nodos. Estos son conocidos como Servidores de la Función Sin Conexión (CLSF). Otro tema con este tipo de servicio se relaciona con el asignamiento de MIDs. Está claro que, si dos nodos fuente utilizan simultáneamente el mismo MID y las tramas son para el mismo destino, el procedimiento de reensamblado no funcionará. En consecuencia, para superar esta eventualidad, el CLSF puede también cambiar el MID durante su operación de retransmisión, si este ya está en uso en un nodo de destino dado.

#### 4.6.2.2.6 Comunicaciones de datos sobre ATM - AAL5 (SEAL).

AAL5 es un protocolo para soportar transmisiones de datos con o sin conexión. Elimina parte de la complejidad y sobrecarga introducida por AAL3/4, proporcionando un nivel de adaptación simple y eficiente para la transmisión de tramas de datos entre dispositivos tales como enrutadores, sobre una red ATM.

AAL5 define un formato de trama de longitud variable, así como los procedimientos para segmentar la trama en celdas para su transmisión sobre la red ATM, y el reensamblado en destino.

El subnivel de convergencia CS, para realizar sus funciones añade 8 bytes por trama: Un CRC para detectar errores de trama y celdas perdidas, 2 bytes de para especificar la longitud de la trama (0-65.535 bytes), 2 bytes de control reservados. Hay un campo de relleno (PAD) conteniendo de 0 a 47 bytes con el fin de el número total de bytes sea múltiplo de 48. La unidad de datos del protocolo así generada (CS-PDU), es transportada al subnivel SAR para su segmentación.

El subnivel SAR utiliza un bit del campo PT de la cabecera de la celda ATM, para indicar que es la última celda (EOM) perteneciente a la trama (PT = 0x1), o no es la última (not EOM, PT = 0x0). No consume ninguna parte de la carga útil de la celda para realizar esta función, obteniéndose una mejora de 4 bytes por celda frente a AAL3/4.

AAL5, a diferencia de AAL3/4, no permite la multiplexación de mensajes de diferentes usuarios (diferentes SDUs) dentro de un mismo VPI/VC1 ya que no contiene el IDentificador de Mensaje (MID), así que requiere un VPI/VC1 dedicado.

#### 4.6.2.3 Ventajas y desventajas que ofrecen estas tecnologías de conexión por medio de circuitos virtuales.

Las tecnologías Frame Relay y ATM pertenecen a las redes de conmutación de paquetes. Por lo tanto se determinarán las ventajas entre estas dos tecnologías.

Frame relay fue creado con la intención de sustituir directamente al estándar X.25. Asumiendo que el transporte de datos a través de la red es muy confiable, Frame Relay elimina la corrección de errores en los nodos intermedios de la red, transfiriéndolo a los extremos de la conexión, es decir, a los protocolos de nivel superior (particularmente, a la capa de transporte). Esto hace que frame relay sea mucho más rápido que X.25, aunque también es más difícil y costoso de implementar. Aunque recientemente se ha comenzado a estudiar la utilización de frame relay para la transmisión de voz y vídeo, en términos generales puede decirse que frame relay fue creado con orientación a la transmisión de datos.

Por otra parte ATM fue creado con la intención de convertirlo en la tecnología de conmutación o modo de transferencia de B-ISDN (*Broadband integrated services digital network*). Desde sus inicios los esfuerzos de los creadores del conjunto de estándares ATM estuvieron orientados a permitir la transmisión de voz, datos y vídeo, por lo que ATM es una tecnología con una orientación de mayor alcance que frame relay.

##### 4.6.2.3.1 Velocidad de acceso.

La diferencia cuantitativa más importante entre Frame Relay y ATM está en las velocidades de acceso y de transmisión de datos que cada uno es capaz de proveer. La interfaz frame relay (FRI o *frame relay interface*) ofrece las siguientes velocidades de acceso principales:

- 56 kbps
- n x 64 kbps

- 
- 1,544 Mbps (T1)
  - 2,048 Mbps (E1)

Algunos fabricantes ofrecen velocidades de acceso para frame relay en el orden de los 45 Mbps, sin embargo, esto no está contemplado en el estándar original.

Por su parte ATM ofrece velocidades de acceso en el rango de 25 Mbps hasta 10 Gbps. Esto nos indica que ATM es capaz de trabajar con anchos de banda más grandes que frame relay. Suele decirse que ATM se mueve en el grupo de las denominadas redes de banda amplia (*broadband networks*) mientras que frame relay está en el grupo de las redes de banda estrecha (*narrowband networks*).

La diferencia tan notable de velocidad entre uno y otro nace fundamentalmente de la unidad de transmisión de datos empleada por cada estándar. Frame relay emplea tramas de tamaño variable, que pueden causar retardos de procesamiento a nivel de los switches de conmutación de la red. Por su parte ATM ofrece una mayor velocidad al emplear una unidad de tamaño fijo denominada celda (53 bytes), lo que simplifica el procesamiento a nivel de los nodos, haciéndolo predecible y eficiente. Algunas ventajas generales de la utilización de celdas en relación a la utilización de tramas son las siguientes:

- Dado que por definición todas las celdas tienen la misma longitud, esto simplifica drásticamente el proceso de conmutación. En general, para una capacidad fija de procesamiento en los nodos y un tiempo igual, se pueden transportar más datos en un sistema basado en celdas que en un sistema basado en tramas.
- El retardo de las celdas en cada nodo de la red es inferior al de los tramas porque la mayoría de las arquitecturas de conmutación requieren que se haya recibido la unidad de datos completa (frame o celda) antes de la conmutación y retransmisión. Dado que este retardo es una función directa del tamaño de la unidad recibida y/o transmitida y que los tramas son en promedio de 10 a 100 veces más grandes que las celdas, el retardo acumulado para los tramas en cada nodo es muy significativo en relación al retardo acumulado para las celdas.
- Su tamaño fijo hace más fácilmente predecible el comportamiento de las celdas que el de los tramas, en particular, el tiempo que cada unidad de datos ocupará las facilidades de transmisión. Esto permite crear más fácilmente prioridades para el tráfico de información. Las aplicaciones multimedia (que trabajan en tiempo real) son particularmente beneficiadas porque los datos sensibles al tiempo o de tiempo real (audio y vídeo) pueden ser transmitidas con una mayor prioridad.

No obstante, los sistemas basados en celdas tienen algunas desventajas inherentes. En particular:

- El overhead (la información adicional a los datos) puede ser mucho mayor. Cada celda y frame requiere una cantidad similar de bits de overhead (unos 5 bits), pero como un frame puede llegar a tener un tamaño equivalente a 100 celdas, el overhead en el caso de las celdas puede llegar a ser mucho más significativo.
- Otro punto importante es que las transmisiones de datos suelen ocurrir en ráfagas, que se prestan mejor para el soporte en tramas. En muchas ocasiones, por ejemplo para transportar datos de redes LAN que usan también tramas, el uso de celdas requiere un proceso de segmentación y reensamblaje que no es requerido en los tramas. Este proceso, aunque simple de realizar, agrega un tiempo de procesamiento adicional para las celdas.

#### 4.6.2.3.2 Consideración de la calidad de servicio.

Por su orientación al soporte de la transmisión de varios medios en forma simultánea, en particular, voz, datos y vídeo, ATM fue creado desde el principio con el concepto de calidad de servicio (QoS o *Quality of Service*) en mente, por que lo que varios estándares dentro de ATM enfocan este aspecto (negociación de la calidad de servicio, ajuste de la calidad de servicio sobre demanda, etc.). ATM ofrece además varias clases de servicio para la transmisión (ya anteriormente mencionadas).

Por su parte, en el estándar original Frame Relay incorpora los aspectos de calidad de servicio sólo de forma muy rudimentaria. Las experiencias recientes en la utilización de Frame Relay para la transmisión de voz están obligando a los diversos fabricantes a incorporar aspectos de manejo de la calidad de servicio en frame relay, sin embargo, no existen estándares aceptados universalmente y cada fabricante resuelve el problema mediante técnicas propias. Esto hace que Frame Relay presente serios inconvenientes para el manejo de medios usualmente incorporados en las nuevas aplicaciones multimediales: voz, vídeo y medios en tiempo real en general.

#### 4.6.2.3.3 Costos y acceso

Aunque las altas velocidades de transmisión de ATM lo convierten en una opción con capacidades por encima de las de Frame relay, los altos costos de los equipos ATM tanto para el acceso a la red como para conmutación han limitado su difusión en los años recientes, en tanto que Frame relay ha obtenido una parte importante del mercado, en particular, aquellos usuarios que requieren conexiones para la transmisión de datos a velocidades no exageradamente altas.

Sin embargo, el aumento de la demanda y el surgimiento de aplicaciones cada vez más exigentes en recursos (Internet, sistemas multimediales en red, realidad virtual, etc.) ha producido una reducción en el valor de los equipos ATM, por lo que se piensa que en muchos casos sustituirán progresivamente a aquellos para Frame Relay.

Otros visualizan una convivencia de ambas tecnologías en la que Frame Relay se emplearía a nivel de la última milla o conexión local del usuario y en las redes de baja velocidad (hasta T1 ó E1) y ATM se emplearía a nivel de la parte central de la red soportando múltiples conexiones Frame Relay. Existen varios esfuerzos en marcha para definir la transferencia o "mapeo" de tramas de Frame Relay a celdas de ATM. Estos son:

- Frame Relay/ATM network interworking.
- ATM DXI (data exchange interface).
- ATM/Frame Relay service interworking.
- FUNI.

#### 4.6.2.3.4 Interconexión de redes LAN.

Frame relay se ha mostrado muy útil en la interconexión de redes LAN (una aplicación con un volumen de negocios muy importante) porque la mayor parte de éstas redes emplean unidades de transmisión de datos de tamaño variable al igual que la trama de frame relay, lo que simplifica la transferencia de datos. En el caso de ATM siempre se han atribuido problemas para esta transferencia debidos al tamaño fijo de las celdas. Por ejemplo, para transportar un frame de Ethernet (64 bytes) se requieren dos celdas ATM de 53 bytes (106 bytes), lo que deja una cantidad de espacio no utilizado. En transmisiones de volúmenes de datos importantes esto significa una gran cantidad de overhead adicional para celdas que transportan muy pocos datos.

#### 4.6.2.4 Tabla comparativa.

A continuación se presenta la siguiente tabla comparativa:

	<b>Enlace dedicado</b>	<b>Frame Relay</b>	<b>ATM</b>
<b>Velocidades de transmisión</b>	64Kbps – 45Mbps	64Kbps – 45Mbps (en el estándar original no se contempla este rango)	25 Mbps – 2,4 Gbps.
<b>Calidad de servicio</b>	Alto	Medio	Alto



Accesibilidad	De última milla(No todas las áreas están cableadas con este tipo de líneas.)	Alto	Medio
Ancho de banda	Grande	Medio	Alto
Costo(renta y equipo)	Alto	Medio	Alto

#### 4.6.3 Conclusiones de los diferentes enlaces existentes.

La línea dedicada o enlace dedicado es una tecnología de conmutación de circuitos y es conveniente emplearlo cuando el volumen de información es bastante y es continuo o permanente. Además una muy buena opción cuando el enlace se desea que sea punto a punto y de gran privacidad.

ATM y Frame Relay son dos tecnologías de paquetes rápidos empleadas con frecuencia en aplicaciones de transmisión de datos. Aunque frecuentemente comparadas en términos económicos únicamente, ambas tecnologías ofrecen otras características particulares que las diferencian, siendo las más importantes: orientación general, velocidad de acceso, manejo de parámetros de calidad de servicio, costos e interconexión de redes LAN.

ATM es más adecuada para aplicaciones y sistemas con altos volúmenes de transmisión de datos de medios combinados, en particular: datos, voz y audio.

Frame relay es más adecuada para sistemas con volúmenes de transmisión de datos convencionales, en particular: datos e interconexión de redes LAN.

#### 4.7 Resumen

En este capítulo se describieron los distintos protocolos WAN existentes, así como la descripción del funcionamiento de los mismos. De la misma forma se mencionaron los diferentes estándares que se manejan para la asignación de la mínima tasa de transmisión.

Por otra parte se mencionaron los diferentes enlaces WAN existentes, así como sus ventajas y desventajas de la tecnología en uso.

---

## Capítulo 5. Red.

### 5.1 Introducción.

Como ya sabemos y como se mencionó anteriormente en el capítulo 1, la capa de red proporciona sus servicios a la capa de transporte, siendo una capa compleja que proporciona conectividad y selección de ruta entre dos sistemas de hosts que pueden estar ubicados en redes geográficamente distintas. Además de ocuparse de aspectos de contabilidad de paquetes, es la responsable de las funciones de conmutación y de llevar a cabo el proceso de lograr que cada máquina de una red se encuentre enlazada o unida a otras redes.

Por ejemplo Internet es un conjunto de tecnologías que permiten interconectar redes muy distintas entre sí. Internet no es dependiente de la máquina ni del sistema operativo utilizado. Como administradores de redes es necesario asegurar que las rutas del sistema estén correctamente configuradas.

De esta manera, podemos transmitir información entre un servidor Unix y una computadora que utilice otro sistema operativo. O entre plataformas completamente distintas como Macintosh, Alpha o Intel. Es más: entre una máquina y otra generalmente existirán redes distintas: redes Ethernet, redes FDDI o incluso enlaces vía satélite. Como vemos, está claro que no podemos utilizar ningún protocolo que dependa de una arquitectura en particular. Lo que estamos buscando es un método de interconexión general que sea válido para cualquier plataforma, sistema operativo y tipo de red. La familia de protocolos que se eligieron para permitir que Internet sea una Red de gran capacidad es TCP/IP. Al mencionar TCP/IP hablamos de una familia de protocolos ya que son muchos los protocolos que la integran, aunque en ocasiones para simplificar hablemos sencillamente del protocolo TCP/IP.

El concepto de red está relacionado con las direcciones IP que se configuren en cada estación de trabajo, no con el cableado. Es decir, si tenemos varias redes dentro del mismo cableado solamente las estaciones de trabajo que permanezcan a una misma red podrán comunicarse entre sí. Para que las estaciones de trabajo de una red puedan comunicarse con los de otra red es necesario que existan enrutadores que interconecten las redes. Un enrutador no es más que un dispositivo que enruta la información por medio de las direcciones IP, una para cada red, que permita el tráfico de paquetes entre sus redes.

La capa de red se encarga de fragmentar cada mensaje en paquetes de datos llamados datagramas IP y de enviarlos de forma independiente a través de la red. Cada datagrama IP incluye un campo con la dirección IP de destino. Esta información se utiliza para *enrutar* los datagramas a través de las redes necesarias que los hagan llegar hasta su destino.

### 5.2 Direccionamiento IP

#### 5.2.1 Direcciones.

Todos los destinos en una red poseen un único identificador que permite a otras máquinas enviar información. Este identificador es llamado usualmente dirección. En algunas tecnologías una dirección identifica una máquina en particular, mientras que en otras, como en el protocolo IP, una dirección identifica un punto de unión a la red, comúnmente llamado interfaz. Una máquina puede tener múltiples interfaces, teniendo una dirección IP por cada una de ellas, las interfaces son por lo general conexiones físicas distintas, pero también pueden ser conexiones lógicas compartiendo una misma interfaz.

#### 5.2.2 Dirección IP.

La dirección IP es el identificador de cada host dentro de su red. Cada host conectado a una red tiene una dirección IP asignada, la cual debe ser distinta a todas las demás direcciones que estén vigentes en ese momento en el conjunto de redes visibles por el host. En el caso de Internet, no puede haber dos estaciones de

trabajo con 2 direcciones IP (públicas) iguales. Pero sí podríamos tener dos estaciones de trabajo con la misma dirección IP siempre y cuando pertenezcan a redes independientes entre sí (sin ningún camino posible que las comuniquen).

Las direcciones IP se clasifican en:

- **Direcciones IP públicas.** Son visibles en todo Internet. Una estación de trabajo con una IP pública es accesible (visible) desde cualquier otra estación de trabajo conectado a Internet. Para conectarse a Internet es necesario tener una dirección IP pública.
- **Direcciones IP privadas (reservadas).** Son visibles únicamente por otros hosts de su propia red o de otras redes privadas interconectadas por routers. Se utilizan en las empresas para los puestos de trabajo. Los ordenadores con direcciones IP privadas pueden salir a Internet por medio de un enrutador (o *proxy*) que tenga una IP pública. Sin embargo, desde Internet no se puede acceder a estaciones de trabajo con direcciones IP privadas.

A su vez, las direcciones IP pueden ser:

- **Direcciones IP estáticas (fijas).** Un host que se conecte a la red con dirección IP estática siempre lo hará con una misma IP. Las direcciones IP públicas estáticas son las que utilizan los servidores de Internet con objeto de que estén siempre localizables por los usuarios de Internet.
- **Direcciones IP dinámicas.** Un host que se conecte a la red mediante dirección IP dinámica, cada vez lo hará con una dirección IP distinta. Las direcciones IP públicas dinámicas son las que se utilizan en las conexiones a Internet mediante un módem. Los proveedores de Internet utilizan direcciones IP dinámicas debido a que tienen más clientes que direcciones IP (es muy improbable que todos se conecten a la vez).

Las direcciones IP están formadas por 4 bytes (32 bits). Se suelen representar de la forma a.b.c.d donde cada una de estas letras es un número comprendido entre el 0 y el 255. Por ejemplo una dirección IP puede ser 124.34.156.45.

Las direcciones IP también se pueden representar de la siguiente manera:

Las tres direcciones siguientes representan a la misma máquina.

128.10.2.30.....(decimal)  
80.0A.02.1E..... (Hexadecimal)  
10000000.00001010.00000010.00011110.....(binario)

Podemos calcular el número de direcciones si realizamos la siguiente operación: 2 elevado a la 32 y obtenemos más de 4000 millones de direcciones distintas. Sin embargo, no todas las direcciones son válidas para asignarlas a los hosts. Las direcciones IP no se encuentran aisladas en Internet, sino que pertenecen siempre a alguna red. Todas las máquinas conectadas a una misma red se caracterizan en que los primeros bits de sus direcciones son iguales. De esta forma, las direcciones se dividen conceptualmente en dos partes: el identificador de red y el identificador de host.



### 5.2.3 Clases de direcciones IP.

Dependiendo del número de hosts que se necesiten para cada red, las direcciones IP se han dividido en las clases primarias A, B y C. La clase D está formada por direcciones que identifican no a un host, sino a un grupo de ellos. Las direcciones de clase E no se pueden utilizar (están reservadas).

Bits	0	1	2	3	4	8	16	24	31	
Clase A	0	Red				Host				
Clase B	1	0	Red			Host				
Clase C	1	1	0	Red				Host		
Clase D	1	1	1	0	grupo de multicast (multidifusión)					
Clase E	1	1	1	1	(direcciones reservadas: no se pueden utilizar)					

- Las direcciones de Clase A usan 7 bits para el número de red dando un total de 126 (128-2) posibles redes de este tipo ya que la dirección 0.0.0.0 se utiliza para reconocer la dirección de red propia y la red 127 es la del lazo interno de la máquina. Los restantes 24 bits son para el número de host –quitando las que son todos los bits a 0 ó a 1 con lo cual tenemos hasta  $2^{24}-2=16,777,216-2=16,777,214$  direcciones-. Son las redes 1.0.0.0 a 126.0.0.0
- Las direcciones de Clase B utilizan 14 bits para la dirección de red (16,384 posibles redes de este tipo) y 16 bits para el host (hasta 65.534 máquinas). Son las redes 128.0.0.0 a 191.255.0.0
- Las direcciones de clase C tienen 21 bits para la red (2,097,152 redes) y 8 bits para el host (254 máquinas). Son las redes 192.0.0.0 a 223.255.255.0
- Las direcciones de clase D están reservadas para multicasting que son usadas por direcciones de host en áreas limitadas.
- Las direcciones de Clase E están reservadas para uso futuro.

Clase	Formato (r=red, h=host)	Número de redes	Número de hosts por red	Rango de direcciones de redes
A	r.h.h.h	128	16,777,214	0.0.0.0 - 127.0.0.0
B	r.r.h.h	16,384	65,534	128.0.0.0 - 191.255.0.0
C	r.r.r.h	2,097,152	254	192.0.1.0 - 223.255.255.0
D	Grupo	-	-	224.0.0.0 - 239.255.255.255
E	no válidas	-	-	240.0.0.0 - 255.255.255.255

### 5.2.4 Direcciones IP especiales y reservadas.

No todas las direcciones comprendidas entre la 0.0.0.0 y la 223.255.255.255 son válidas para un host: algunas de ellas tienen significados especiales. Los principales direcciones especiales se resumen en la siguiente tabla. Su interpretación depende del host desde el que se utilicen.

Bits de red	Bits de host	Significado	Ejemplo
todos 0		Mi propio host	0.0.0.0
Todos 0	Host	Host indicado dentro de mi red	0.0.0.10
Red	Todos 0	Red indicada	192.168.1.0

todos 1		Difusión a mi red	255.255.255.255
Red	Todos 1	Difusión a la red indicada	192.168.1.255
127	cualquier valor válido de host	Loopback (mi propio host)	127.0.0.1

**Difusión (broadcast) y multidifusión (multicast).**— El término difusión (broadcast) se refiere a todos los hosts de una red; multidifusión (multicast) se refiere a varios hosts (aquellos que se hayan suscrito dentro de un mismo grupo). Siguiendo esta misma terminología, en ocasiones se utiliza el término unidifusión (unicast) para referirse a un único host.

Difusión o broadcasting es el envío de un mensaje a todas las estaciones de trabajo que se encuentran en una red. La dirección de loopback (normalmente 127.0.0.1) se utiliza para comprobar que los protocolos TCP/IP están correctamente instalados en nuestra propia estación de trabajo.

Las direcciones de redes siguientes se encuentran reservadas para su uso en redes privadas. Una dirección IP que pertenezca a una de estas redes se dice que es una dirección IP privada.

Clase	Rango de direcciones reservadas de redes
A	10.0.0.0
B	172.16.0.0 - 172.31.0.0
C	192.168.0.0 - 192.168.255.0

**Intranet.**— Red privada que utiliza los protocolos TCP/IP. Puede tener salida a Internet o no. En el caso de tener salida a Internet, el direccionamiento IP permite que los hosts con direcciones IP privadas puedan salir a Internet mediante un proxy o un equipo NAT pero impide el acceso a los hosts internos desde Internet. Dentro de una intranet se pueden configurar todos los servicios típicos de Internet (web, correo, mensajería instantánea, etc.) mediante la instalación de los correspondientes servidores. La idea es que las intranets son como "internets" en miniatura o lo que es lo mismo, Internet es una intranet pública gigantesca.

**Extranet.**— Unión de dos o más intranets. Esta unión puede realizarse mediante líneas dedicadas (RDSI, X.25, frame relay, punto a punto, etc.) o a través de Internet.

### 5.2.5 Máscara de subred.

Una máscara de subred es aquella dirección que enmascarando nuestra dirección IP, nos indica si otra dirección IP pertenece a nuestra subred o no. Cada dirección tiene una máscara de red asociada, la cual es representada por un número de 32 bits, donde todos los bits de la porción de red están en 1 y todos los bits de la porción de host están en 0. Por

Ejemplo:

11111111 11111111 00000000 00000000 .....255.255.0.0

En el ejemplo anterior los primeros 16 bits están asociados al número de red y los 16 restantes al número de la máquina dentro de la red.

**TESIS CON  
FALLA DE ORIGEN**

Al igual que las direcciones IP, las máscaras se representan con dotted quat, hexadecimal y una notación adicional llamada dirección base/conteo de bit. Ejemplo la red 192.168.10.0/23.

Clase	Máscara de subred
A	255.0.0.0
B	255.255.0.0
C	255.255.255.0

Formato	Visualización de formato
Terminal ip máscara - Formato decimal	192.168.2.0 255.255.254.0
Terminal ip máscara - Formato hexadecimal	192.168.2.0 0xFFFE00
Terminal ip máscara - Formato cuenta de bit	192.168.2.0/23

### 5.2.6 Formas de dividir una red en subredes(subneteo)

Hay dos formas de dividir una red en subredes: usando longitud estática y longitud variable en la máscara..

Una subred que necesita dividirse en otras dos puede hacerlo añadiendo un bit a su máscara sin afectar al resto. La longitud estática implica que todas las subredes deben tener la misma máscara lo que obligará a poner la máscara que necesite más estaciones de trabajo.

#### 5.2.6.1 Máscara de Subred de Longitud Variable (VLSM):

VLSM permite usar máscaras de subred de longitud variable y diferente a las redes classfull, lo que permite segmentar este tipo de redes.

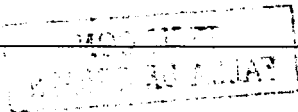
#### Ventajas:

- **Uso aún más eficiente de las direcciones IP:** Sin el uso de las VLSM, las empresas están bloqueadas en la implementación de una sola máscara de red de Clase A, B o C: Usando VLSM la red 172.16.0.0/16 puede ser dividida en subredes que utilizan el enmascaramiento /24, y a su vez una de las subredes de este intervalo, 172.16.14.0/24, se puede dividir aún más en subredes más pequeñas con el enmascaramiento /27.
- **Mayor capacidad de usar la sumarización de ruta:** Las VLSM permite que haya más niveles jerárquicos en el plan de direccionamiento, por lo que permiten un resumen de ruta mejor en las tablas de enrutamiento.

Entonces las VLSM se suelen usar para maximizar el número de direcciones posibles disponibles en una red. Por ejemplo, dado que las líneas seriales de punto a punto sólo requieren dos direcciones de host puede usar una dirección de subred que sólo contenga dos direcciones de host(30 bits), y no derrochar así los números de subred.

A continuación mostramos un ejemplo usando VLSM:

Se pueden agregar bits adicionales a las máscaras de red primarias, con objeto de generar subredes. Cuando se ejecuta la operación AND entre las IP de red y la máscara configurada, se obtiene la dirección de su red. Hay algunas restricciones en las direcciones de red. Las direcciones de nodo de todos "0" o todos "1", están



reservadas para especificar la red local y la red de broadcast. Estas restricciones implican que no puede utilizarse solo un bit para generar subredes.

Calcular las subredes generadas en la red 140.179.0.0 y el espacio de direccionamiento utilizable, si se emplea una máscara de subred de 255.255.224.0.

Para resolver el problema, vamos a determinar cuantos bits se utilizaron para generar subredes.

140.179.0.0.....en binario es 10001100.10110011.00000000.00000000 .....IP de red.

255.255.224.0.....en binario es 11111111.11111111.11000000.00000000.....máscara configurada

En este ejemplo se utilizan 3 bits para formar las subredes con VLSM.

Para encontrar los números de subred, en la red Clase B 140.179.0.0, hacemos variar los primeros 3 bits de esta dirección a todas las combinaciones posibles, ya que se emplearon 3 bits para subneteo eso es debido a la máscara que se utilizó en este ejemplo.

Subred 0	10001100.10110011.00000000.00000000	este valor en decimal es 140.179.0.0
Subred 1	10001100.10110011.00100000.00000000	este valor en decimal es 140.179.32.0
Subred 2	10001100.10110011.01000000.00000000	este valor en decimal es 140.179.64.0
Subred 3	10001100.10110011.01100000.00000000	este valor en decimal es 140.179.96.0
Subred 4	10001100.10110011.10000000.00000000	este valor en decimal es 140.179.128.0
Subred 5	10001100.10110011.10100000.00000000	este valor en decimal es 140.179.160.0
Subred 6	10001100.10110011.11000000.00000000	este valor en decimal es 140.179.192.0
Subred 7	10001100.10110011.11100000.00000000	este valor en decimal es 140.179.224.0

Por restricciones en los equipos de comunicación, las subredes con todos "0" o "1" en el campo de subred no pueden utilizarse. De acuerdo con esto, la Subred 0 y la subred 7, no pueden utilizarse.

Para encontrar las direcciones de broadcast de estas subredes, establecemos a 1 los bits del campo de host en las subredes.

Subred 0	10001100.10110011.00011111.11111111	broadcast es 140.179.31.255
Subred 1	10001100.10110011.00111111.11111111	broadcast es 140.179.63.255
Subred 2	10001100.10110011.01011111.11111111	broadcast es 140.179.95.255
Subred 3	10001100.10110011.01111111.11111111	broadcast es 140.179.127.255
Subred 4	10001100.10110011.10011111.11111111	broadcast es 140.179.159.255
Subred 5	10001100.10110011.10111111.11111111	broadcast es 140.179.191.255
Subred 6	10001100.10110011.11011111.11111111	broadcast es 140.179.223.255
Subred 7	10001100.10110011.11111111.11111111	broadcast es 140.179.255.255

Descartamos las direcciones de subred y de broadcast, y el espacio de direccionamiento restante, es nuestro direccionamiento utilizable.

Subred 1	140.179.0.1 - 140.179.31.254
Subred 2	140.179.32.1 - 140.179.63.254
Subred 3	140.179.64.1 - 140.179.95.254
Subred 4	140.179.96.1 - 140.179.127.254
Subred 5	140.179.128.1 - 140.179.159.254
Subred 6	140.179.160.1 - 140.179.191.254
Subred 7	140.179.192.1 - 140.179.223.254
Subred 8	140.179.224.1 - 140.179.255.254

En este ejemplo se utilizó una máscara de subred de 3 bits. Hay 6 subredes disponibles y cada subred cuenta con 8190 nodos. Esto da un total de 49140 nodos en esta red de clase B.

### 5.2.6.2 Direccionamiento sin clase CIDR (Classless Inter – Domain Routing)

El esquema de Direcciones sin Clase, que consiste en asignar a una misma organización un bloque continuo de direcciones IP. De esta manera, una organización que requiera conectar a Internet un numero moderado de Hosts (digamos 3,800) puede recibir un bloque de 16 redes continuas Clase C (por ejemplo, de la red Clase C 199.40.72.0 a la 199.40.87.0), con lo cual dispone de 4.096 direcciones IP validas para administrar. El esquema de direcciones con clase genera el problema de aumentar la información que debe incluirse en las tablas de enrutamiento. En el caso del ejemplo, se tendría que incluir 16 nuevas entradas en cada tabla de enrutamiento de cada Host y enrutador. CIDR resuelve el problema al incluir en las tablas información acerca del tamaño de los bloques y el numero de bloques, así, en las tablas de enrutamiento IP se tienen pares (Destino, enrutador), donde destino no es una dirección de Host o Red tradicional, sino que incluye información acerca del numero de redes que incluye el bloque. El Direccionamiento sin clase modifica la estructura de una dirección IP, de esta manera:

Prefijo de Red	Identificador de Host
----------------	-----------------------

Así, CIDR debe incluir en las tablas de enrutamiento cual es la primera red que compone el bloque, cuantos bits se emplean como Prefijo de Red y la mascara de subred que se emplea. En nuestro ejemplo, las tablas de enrutamiento IP contendrían esta información:

```

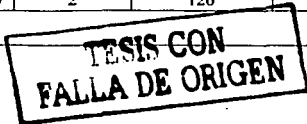
199.40.72.0/20 ..... 11000111.10100000.10010000.00000000
255.255.240.0 ..... 11111111.11111111.11110000.00000000
  
```

Refiriéndose a un bloque que se inicia con la red 199.40.72.0 y que tiene 20 bits en el prefijo de red. La mascara 255.255.240.0 (11111111.11111111.11110000.00000000) nos indica que se están usando 4 bits extra (los que se han resaltado) para identificar a las redes que componen al bloque. Podemos ver que cuatro bits permiten agrupar precisamente 16 redes Clase C.

Un aspecto importante que hay que subrayar es que en ningún momento cambia el algoritmo básico de enrutamiento IP, lo que cambia es el contenido de las tablas. Además, las nuevas tablas contienen información resumida, por lo que buscar una dirección destino en la tabla se hace de otra manera, pero el algoritmo permanece inalterado.

El problema de buscar direcciones de destino en una tabla, consiste en que cualquier dirección cuya mascara de destino tenga menos bits, incluye a la que tiene mas bits. Con dar a entender que una mascara de subred como 255.255.0.0 (11111111.11111111.00000000.00000000), es decir, 16 bits de prefijo de red) incluye dentro de sí a las mascaras de subred 255.255.128.0 (11111111.11111111.10000000.00000000), 17 bits de prefijo de red) y esta a su vez incluye a la mascara 255.255.192.0 (11111111.11111111.11000000.00000000) y en general, entre menos bits tiene el prefijo de red, mas direcciones Host abarca. Por esta razón cuando se explora la tabla de enrutamiento IP en busca de una dirección de destino, se hace una búsqueda que inicia con las mascaras de más bits y termina en la de menos bits. Es decir, se inicia con mascaras como 255.255.255.255 (todo en uno) y se continua con la 255.255.255.254 (31 unos y un cero) y así sucesivamente.

Máscara de subred	Binario	Número de subredes	Núm. de hosts por subred	Ejemplos de subredes (x=a.b.c por ejemplo, 192.168.1)
255.255.255.0	00000000	1	254	x.0
255.255.255.128	10000000	2	126	x.0, x.128





255.255.255.192	11000000	4	62	x.0, x.64, x.128, x.192
255.255.255.224	11100000	8	30	x.0, x.32, x.64, x.96, x.128, ...
255.255.255.240	11110000	16	14	x.0, x.16, x.32, x.48, x.64, ...
255.255.255.248	11111000	32	6	x.0, x.8, x.16, x.24, x.32, x.40, ...
255.255.255.252	11111100	64	2	x.0, x.4, x.8, x.12, x.16, x.20, ...
255.255.255.254	11111110	128	0	ninguna posible
255.255.255.255	11111111	256	0	ninguna posible

### 5.2.7 Protocolo IP.

IP es el principal protocolo de la capa de red. Este protocolo define la unidad básica de transferencia de datos entre el origen y el destino, atravesando toda la red de redes. Además, el software IP es el encargado de elegir la ruta más adecuada por la que los datos serán enviados. Se trata de un sistema de entrega de paquetes (llamados *datagramas IP*) que tiene las siguientes características:

- Es no orientado a conexión debido a que cada uno de los paquetes puede seguir rutas distintas entre el origen y el destino. Entonces pueden llegar duplicados o desordenados.
- Es no fiable porque los paquetes pueden perderse, dañarse o llegar retrasados.

### 5.2.8 Formato del datagrama IP.

El datagrama IP es la unidad básica de transferencia de datos entre el origen y el destino. Viaja en el campo de datos de las tramas físicas (trama Ethernet) de las distintas redes que va atravesando. Cada vez que un datagrama tiene que atravesar un enrutador, el datagrama saldrá de la trama de enlace de la red que abandona y se acomodará en el campo de datos de una trama de enlace de la siguiente red. Este mecanismo permite que un mismo datagrama IP pueda atravesar redes distintas: enlaces punto a punto, redes ATM, redes Ethernet, etc. El propio datagrama IP tiene también un campo de datos: será aquí donde viajan los paquetes de las capas superiores.

0	1	2	3	4	5	6	7	0	1	2	3	4	5	6	7	0	1	2	3	4	5	6	7								
VERS								IHL								Tipo de servicio								Longitud total							
Identificación								Protocolo								Banderas				Desplazamiento de fragmento				CRC cabecera							
TTL																															
Dirección IP origen																															
Dirección IP destino																															
Opciones IP (si las hay)																Relleno															
Datos																															

Campos del datagrama IP:

<b>VERS (4 bits).</b>	Indica la versión del protocolo IP que se utilizó para crear el datagrama. Actualmente se utiliza la versión 4 (IPv4) aunque ya se están preparando las especificaciones de la siguiente versión, la 6 (IPv6).
<b>IHL (4 bits).</b>	Longitud de la cabecera expresada en múltiplos de 32 bits. El valor mínimo es 5, correspondiente a 160 bits = 20 bytes.
<b>Tipo de servicio (8bits).</b>	Los 8 bits de este campo se dividen a su vez en: <ul style="list-style-type: none"> <li>• <b>Prioridad (3 bits).</b> Un valor de 0 indica baja prioridad y un valor de 7, máxima.</li> <li>• Los siguientes tres bits indican cómo se prefiere que se transmita el mensaje, es decir, son sugerencias a los encaminadores que se</li> </ul>

	<ul style="list-style-type: none"> <li>• encuentren a su paso los cuales pueden tenerlas en cuenta o no.</li> <li>• <b>Bit D (Delay)</b>. Solicita retardos cortos (enviar rápido).</li> <li>• <b>Bit T (Throughput)</b>. Solicita un alto rendimiento (enviar mucho en el menor tiempo posible).</li> <li>• <b>Bit R (Reliability)</b>. Solicita que se minimice la probabilidad de que el datagrama se pierda o resulte dañado (enviar bien).</li> <li>• Los siguientes dos bits no tienen uso.</li> </ul>
<b>Longitud total</b> (16 bits).	Indica la longitud total del datagrama expresada en bytes. Como el campo tiene 16 bits, la máxima longitud posible de un datagrama será de 65535 bytes.
<b>Identificación</b> (16 bits).	Número de secuencia que junto a la dirección origen, dirección destino y el protocolo utilizado identifica de manera única un datagrama en toda la red. Si se trata de un datagrama fragmentado, llevará la misma identificación que el resto de fragmentos.
<b>Banderas</b> (3 bits).	Sólo 2 bits de los 3 bits disponibles están actualmente utilizados. El bit de <i>Más fragmentos</i> (MF) indica que no es el último datagrama. Y el bit de <i>No fragmentar</i> (NF) prohíbe la fragmentación del datagrama. Si este bit está activado y en una determinada red se requiere fragmentar el datagrama, éste no se podrá transmitir y se descartará.
<b>Desplazamiento de fragmentación</b> (13 bits)	Indica el lugar en el cual se insertará el fragmento actual dentro del datagrama completo, medido en unidades de 64 bits. Por esta razón los campos de datos de todos los fragmentos menos el último tienen una longitud múltiplo de 64 bits. Si el paquete no está fragmentado, este campo tiene el valor de cero.
<b>Tiempo de vida o TTL</b> (8 bits).	Número máximo de segundos que puede estar un datagrama en la red. Cada vez que el datagrama atraviesa un enrutador se resta 1 a este número. Cuando llegue a cero, el datagrama se descarta y se devuelve un mensaje ICMP de tipo "tiempo excedido" para informar al origen de la incidencia.
<b>Protocolo</b> (8 bits).	Indica el protocolo utilizado en el campo de datos: 1 para ICMP, 2 para IGMP, 6 para TCP y 17 para UDP.
<b>CRC cabecera</b> (16 bits).	Contiene la suma de comprobación de errores sólo para la cabecera del datagrama. La verificación de errores de los datos corresponde a las capas superiores.
<b>Dirección origen</b> (32 bits).	Contiene la dirección IP del origen.
<b>Dirección destino</b> (32 bits).	Contiene la dirección IP del destino.
<b>Opciones IP.</b>	Este campo no es obligatorio y especifica las distintas opciones solicitadas por el usuario que envía los datos (generalmente para pruebas de red y depuración).
<b>Relleno.</b>	Si las opciones IP (en caso de existir) no ocupan un múltiplo de 32 bits, se completa con bits adicionales hasta alcanzar el siguiente múltiplo de 32 bits (recuérdese que la longitud de la cabecera tiene que ser múltiplo de 32 bits).
<b>Datos</b>	Contiene la información del datagrama.

### 5.2.9 Fragmentación MTU (Maximum Transfer Unit).

Ya hemos visto que las tramas físicas tienen un campo de datos y que es aquí donde se transportan los datagramas IP. Sin embargo, este campo de datos no puede tener una longitud indefinida debido a que está limitado por el diseño de la red. El MTU de una red es la mayor cantidad de datos que puede transportar su trama física. El MTU de las redes Ethernet es 1500 bytes. Esto significa que una red Ethernet nunca podrá transportar un datagrama de más de 1500 bytes sin fragmentarlo.

Un enrutador fragmenta un datagrama en varios si el siguiente tramo de la red por el que tiene que viajar el datagrama tiene un MTU inferior a la longitud del datagrama. Veamos con el siguiente ejemplo cómo se produce la fragmentación de un datagrama (ver figura 5.2.1.10.1).



Figura 5.2.1.9.1 Ejemplo de fragmentación

Supongamos que el host A envía un datagrama de 1400 bytes de datos (1420 bytes en total) al host B. El datagrama no tiene ningún problema en atravesar la red 1 ya que  $1420 < 1500$ . Sin embargo, no es capaz de atravesar la red 2 ( $1420 >= 620$ ). El enrutador R1 fragmenta el datagrama en el menor número de fragmentos posibles que sean capaces de atravesar la red 2. Cada uno de estos fragmentos es un nuevo datagrama con la misma *Identificación* pero distinta información en el campo de *Desplazamiento de fragmentación* y el bit de *Más fragmentos (MF)*. Veamos el resultado de la fragmentación:

**Fragmento 1:** Long. Total = 620 bytes; Desp = 0; MF=1 (contiene los primeros 600 bytes de los datos del datagrama original)

**Fragmento 2:** Long. Total = 620 bytes; Desp = 600; MF=1 (contiene los siguientes 600 bytes de los datos del datagrama original)

**Fragmento 3:** Long. Total = 220 bytes; Desp = 1200; MF=0 (contiene los últimos 200 bytes de los datos del datagrama original)

El enrutador R2 recibirá los 3 datagramas IP (fragmentos) y los enviará a la red 3 sin reensamblarlos. Cuando el host B reciba los fragmentos, recompondrá el datagrama original. Los enrutadores intermedios no reensamblan los fragmentos debido a que esto supondría una carga de trabajo adicional, a parte de memorias temporales. Nótese que el host destino puede recibir los fragmentos cambiados de orden pero esto no supondrá ningún problema para el reensamblado del datagrama original puesto que cada fragmento guarda suficiente información.

Si el datagrama del ejemplo hubiera tenido su bit *No fragmentar (NF)* a 1, no hubiera conseguido atravesar el enrutador R1 y, por tanto, no tendría forma de llegar hasta el host B. El enrutador R1 descartaría el datagrama.

### 5.3 Protocolos de Enrutamiento

Los protocolos de enrutamiento determinan las rutas que siguen los protocolos enrutados hacia los destinos. Entre los ejemplos de protocolos de enrutamiento se pueden incluir el Protocolo de Información de

---

Enrutamiento (RÍP), el Protocolo de Enrutamiento de Gateway Interior (IGRP), el Protocolo de Enrutamiento de Gateway Interior Mejorado (EIGRP) y el Primero la ruta libre más corta(OSPF) .

Los protocolos de enrutamiento permiten que los enrutadores conectados creen un mapa interno de los demás enrutadores de la red o de Internet. Esto permite que se produzca el enrutamiento (es decir, la selección de la mejor ruta y conmutación). Estos mapas forman parte de la tabla de enrutamiento de cada enrutador.

### 5.3.1.1 Routing information Protocol (RIP)

El protocolo más simple y antiguo fue introducido en Berkeley para mantener tablas correctas en sus redes locales. Nunca fue concebido como un protocolo escalable de enrutamiento, hasta la fecha se usa bastante en redes pequeñas. La idea es mantener en la tabla de enrutamiento, además de la red y el gateway (que simplemente es ruta de salida por defecto), una métrica que cuente la distancia a la que se encuentra el host de esa red. De esta forma, al recibir otras posibles rutas a la misma red, puede elegir la más corta. RIP es un protocolo de vector distancia, donde cada enrutador puede verse como un nodo, y las distancias son el número de nodos por los que debe pasar para llegar a su destino. Cada enrutador maneja su tabla de enrutamiento, donde figuran todos los nodos de la red y la distancia asociada. Cada cierto tiempo, los enrutadores envían esa tabla completa a todos sus vecinos. Al recibir la tabla de otro enrutador, aprende los caminos a redes que no conocía (y los agrega a su tabla) y encuentra nuevos caminos a redes que ya conocía. Para elegir una ruta, compara las métricas (al recibir una tabla, le suma 1 a todas sus métricas, puesto que las redes están a un enrutador más de distancia) y se queda con la más pequeña. En caso de igualdad, se queda con la ruta antigua, para evitar cambios permanentes en las rutas. Además de las rutas aprendidas por RIP, típicamente se maneja una ruta default, y las rutas directas a las redes a las que está conectado el enrutador, cuyas métricas son cero. Para encontrar a los demás enrutadores y poder intercambiar con ellos las tablas, RIP utiliza un esquema de broadcast. Un enrutador que habla RIP, difunde vía broadcast a todas las redes a las que está conectado su tabla de rutas periódicamente. Al recibir un broadcast RIP, el enrutador compara sus entradas con las recibidas y actualiza la tabla. Sin embargo, para poder adaptarse a fallas o caídas de enrutadores, debe poder realizar el borrado de rutas. Como no puede confiarse que el enrutador caído avise, se define un intervalo de tiempo fijo entre broadcasts, que en RIP por defecto es de 30 seg. Al transcurrir varios intervalos sin escuchar nada de un enrutador (180 seg.) todas las rutas que fueron recibidas desde él se invalidan. RIP tiene varias ventajas, probablemente la principal es que funciona prácticamente sólo, sin necesidad de configuración o ingeniería inicial. Basta habilitar RIP en el enrutador, y éste aprende y difunde todas las rutas automáticamente. Esta misma sencillez es su principal defecto, puesto que satura la red con broadcasts innecesarios y utiliza métricas que no toman en cuenta capacidades de las distintas redes. El principal problema de RIP es un defecto fundamental de cualquier protocolo de vector de distancias: al manejar sólo distancias, no puedo detectar los loops en las rutas. Al cambiar las rutas, es fácil caer en ciclos infinitos. Para evitar el problema de los loops infinitos, en RIP se define que una métrica 16 es equivalente a infinito. Además, se implementan otras soluciones que son:

**Horizontes Divididos (Split Horizon):** un enrutador no anuncia rutas por la misma interfaz en que le llegaron. Con esto se elimina el problema de tener que contar hasta el infinito (16).

**Envenenamiento en Reverso (Poison Reverse):** cuando un enlace se cae, el enrutador inmediatamente envía un mensaje con la ruta y una distancia de infinito (16).

**Actualizaciones Inmediatas (Triggered Updates):** cuando uno de los enlaces de un enrutador se cae, un mensaje de actualización es enviado sin necesidad de esperar los 30 s reglamentarios.

**Espera (Hold Down):** cuando un enrutador detecta que un enlace se ha caído, este no acepta mensajes de enrutamiento por un período determinado. Esto permite que la actualización inmediatamente se propague.

#### 5.3.1.1.1 Estructura del Frame de RIP

**TRABAJE CON  
FALLA DE ORIGEN**

Comando	Versión	0
AFI		0
Dirección		
0		
0		
Métrica		
Comando	Versión	No Usado
AFI		Etiqueta Ruta/Tipo Autenticación
Dirección/Autenticación		
Máscara de Subred/Autenticación		
Siguiete Salto/Autenticación		
Métrica/Autenticación		

Estructura de un paquete a) RIP b) RIPv2.

Figura 5.3.1.1.1.1 Estructura de paquete

La Figura ilustra el formato de un paquete RIP, la descripción de los campos de las 2 versiones de RIP es la siguiente:

<b>Comando.</b>	1 Byte que indica si el paquete es una petición o respuesta. La petición es una solicitud a un enrutador para que envíe toda o parte de su tabla, información que estará contenida en un paquete de respuesta.
<b>Versión.</b>	1 Byte especificando la versión del protocolo.
<b>Cero.</b>	Dos campos de 2 Bytes y dos de 4 Bytes, no utilizados cuyo valor es cero.
<b>AFI.</b>	2 Bytes que especifica la familia de la dirección utilizada, lo que permite transportar diversos protocolos.
<b>Dirección.</b>	4 Bytes para la dirección de red de cada entrada de la tabla de enrutamiento.
<b>Métrica.</b>	4 Bytes que indican el número de saltos. Su valor puede ir entre 1 y 15.
<b>Formato del Frame de RIP v2.</b>	
<b>Comando.</b>	1 Byte que indica si el paquete es una petición o respuesta. La petición es una solicitud a un enrutador para que envíe toda o parte de su tabla, información que estará contenida en un paquete de respuesta.
<b>Versión.</b>	1 Byte especificando la versión 2 del protocolo.
<b>No Usado.</b>	2 Bytes no utilizados cuyo valor es cero.

<b>AFI.</b>	2 Byte que especifica la familia de la dirección utilizada, lo que permite transportar diversos protocolos. Este campo presenta una pequeña diferencia con la versión anterior de RIP, si el valor es 0xFFFF, entonces el paquete enviado no contiene tablas, sino que es un paquete de autenticación, por lo que el campo de 2 Bytes siguiente pasa a llamarse Tipo de Autenticación y los 16 Bytes siguientes a éste se llaman Autenticación.
<b>Etiqueta de Ruta.</b>	2 Bytes que permiten distinguir si las rutas son internas, es decir, aprendidas por RIP o externas, que son aquellas aprendidas desde otros protocolos.
<b>Tipo de Autenticación.</b>	En el caso de que el campo AFI indique que se trata de un paquete de autenticación, el campo Etiqueta de Ruta toma este nombre. Puede ser texto plano o MD5.
<b>Dirección.</b>	4 Bytes para dirección de red de cada entrada de la tabla de enrutamiento.
<b>Máscara de Subred.</b>	4 Bytes que contienen la máscara de subred. En el caso de que el valor sea 0, entonces no se ha especificado una máscara.
<b>Siguiente Salto.</b>	4 Bytes para indicar la dirección del siguiente salto al cual los paquetes deben ser reenviados.
<b>Métrica.</b>	4 Bytes que indican el número de saltos. Su valor puede ir entre 1 y 16.
<b>Autenticación.</b>	16 Bytes que permiten ingresar un password, en texto plano, para la autenticación. Este campo permite un máximo de 16 caracteres para el password, los cuales son rellenados con ceros hasta completar los 16 en caso de ser menor. Al igual que en el caso anterior, hasta 25 entradas pueden indicarse en un paquete IP.

### 5.3.1.2 Protocolo RIP v2.

El protocolo RIP versión 2 se desarrolló para mejorar el desempeño de las redes basadas en este protocolo y para corregir las limitaciones de la versión 1 de RIP. Los principales cambios se mencionan a continuación;

- Soporte a redes configuradas con VLSM.
- Mecanismos de autenticación.
- Soporte a transmisión en multicast.
- Sumarización de rutas automáticas (desactivable).

### 5.3.2 Interior Gateway Routing Protocol (IGRP)

Con la creación de IGRP a principios de los ochentas, Cisco Systems fue la primera compañía en resolver los problemas asociados con el uso de RIP para enrutar paquetes entre enrutadores interiores. IGRP determina la mejor ruta a través de una red examinando el ancho de banda y la demora de las redes entre los enrutadores. IGRP converge más rápido que RIP, por lo tanto se evitan los loops de enrutamiento causados por el desacuerdo entre enrutadores sobre cual es el próximo salto a ser tomado. Más aún, el IGRP no tiene limitación en cuanto a contador de saltos. Por lo anterior, el IGRP es utilizado en redes de mediano tamaño y con diversidad de topologías. IGRP utiliza una métrica compuesta que es calculada por una suma ponderada de los valores de retardo entre redes, ancho de banda del enlace, confiabilidad y carga, donde el

administrador de la red puede dar valores arbitrarios para las ponderaciones, lo que permite un grado mayor de flexibilidad. Una característica adicional de IGRP es que permite enrutamiento multitrayectoria, lo que permite, por ejemplo, establecer líneas de respaldo en caso de fallas. Para mejorar la estabilidad del algoritmo de vector de distancias, IGRP utiliza mensajes Holddown que evitan que las actualizaciones regulares enviadas por los enrutadores comiencen el problema de la cuenta hasta infinito, ya que al detectar una falla, debido a la falta de actualizaciones, un enrutador que detecte esto envía el mensaje Holddown para evitar que comiencen las sucesivas actualizaciones y se genere la cuenta hasta infinito. Este mensaje es un período de tiempo en el que no deben actualizarse las rutas recibidas. IGRP también utiliza las técnicas Split Horizon y Poison-Reverse en el envío de actualizaciones para prevenir loops información entre enrutadores adyacentes. Finalmente, IGRP mantiene una serie de timers e intervalos de tiempo, entre los que se incluye un timer para actualizaciones o Updates (cuyo valor por defecto es 90 seg.), uno para marcar las rutas como no válidas (por defecto  $3 * \text{Update} = 270$  seg.), uno para el tiempo de Holddown (por defecto  $3 * \text{Update} + 10 = 280$  seg.) y uno para el de descarte de rutas (por defecto  $7 * \text{Update} = 630$  seg.)

Algunas de las características de diseño claves de IGRP enfatizan lo siguiente: · versatilidad que permite manejar automáticamente topologías indefinidas y complejas · flexibilidad para segmentos con distintas características de ancho de banda y de retardo · escalabilidad para operar en redes de gran envergadura El protocolo de enrutamiento IGRP utiliza por defecto dos métricas, ancho de banda y retardo. IGRP puede utilizar una combinación de variables para determinar una métrica compuesta. Estas variables incluyen: · ancho de banda · retardo · carga · confiabilidad

### 5.3.3 Protocolo OSPF (Open Shortest Path First).

#### 5.3.3.1 El protocolo OSPF

Es un protocolo de estado de enlace que utiliza el algoritmo SPF para crear las bases de datos de la topología de la red. Las ventajas que ofrece este protocolo hacen que los administradores lo implementen en redes IP complejas y de gran tamaño.

El protocolo OSPF propone el uso de rutas más cortas y accesibles mediante la construcción de un mapa de la red y mantenimiento de bases de datos con información sobre sistemas locales y vecinos, de esta manera es capaz de calcular la métrica para cada ruta, entonces se eligen las rutas de enrutamiento más cortas. En este proceso se calculan tanto las métricas de estado del enlace como de distancia, en el caso de RIP se calcula sólo la distancia y no el tráfico del enlace, por esta causa OSPF es un protocolo de enrutamiento diseñado para redes con crecimiento constante y capaz de manejar una tabla de enrutamiento distribuida y de rápida propagación, algunas de las características más sobresalientes de OSPF están:

- Rápida detección de cambios en la topología y restablecimiento muy rápido de rutas.
- Poca sobrecarga, usa actualizaciones que informan de los cambios de rutas.
- División de tráfico por varias rutas equivalentes.
- Enrutamiento según el tipo de servicio.
- Uso de multi-envío en las redes de área local.
- Mascaras de subred.
- Autenticación.

La topología de una red OSPF se basa en el concepto de área. Como se muestra en la figura siguiente, la red OSPF esta organizada en áreas dentro del mismo sistema autónomo, todos los enrutadores pertenecientes a una misma área mantienen una copia de la topología de la red.

TESIS CON  
FALLA DE ORIGEN

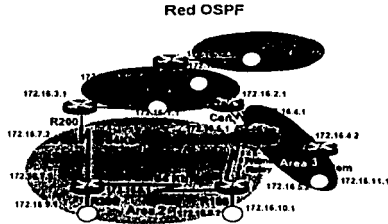


Figura 5.3.3.1.1 Red OSPF

### 5.3.3.2 Áreas y Dominio de enrutamiento OSPF.

En el ámbito de OSPF, el término *red* significa una red IP. Un área es un conjunto de redes y host contiguos, junto con cualesquiera enrutadores con interfaces a estas redes. Un sistema autónomo que use OSPF está construido por una o más áreas. Cada área tiene asignado un número. El área 0 está conectada al Backbone que enlaza con el resto de áreas y agrupa al resto de sistemas autónomos (ver figura 5.3.3.2.1). Cada área ejecuta una copia separada del algoritmo de enrutamiento básico Shortest Path First (SPF), lo que implica que cada área tiene su propia base de datos topológica. La topología de un área es invisible para cualquier dispositivo que no pertenezca a ella. Es decir, los enrutadores internos de algún área específica no saben nada de la topología externa al área. Este aislamiento es la que permite introducir un bajo tráfico de enrutamiento en la red, en comparación a la idea de compartir toda la información del sistema autónomo. Los enrutadores que están conectados a múltiples áreas son llamados *enrutadores de borde de área (ABR)*. Es así como dos enrutadores que pertenecen a una misma área tienen, para esa área, una base de datos idéntica. El enrutamiento en un sistema autónomo tiene dos niveles, dependiendo de si la fuente y el destino están en una misma área o no. El *enrutamiento intraárea* pertenece al primer caso, los paquetes son enrutados con información exclusivamente del área en cuestión. Esto protege al enrutamiento de la inyección de información corrupta. En el *enrutamiento interárea*, se obtiene información del o las áreas exteriores involucradas.

TESIS CON  
FALLA DE ORIGEN

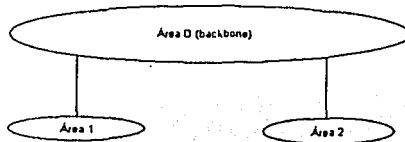


Figura 5.3.3.2.1 Sistema OSPF.



### 5.3.3.3 Backbone OSPF.

Todo dominio de enrutamiento OSPF debe tener un backbone. El backbone es un área especial que tiene un identificador 0.0.0.0, o simplemente 0, y consiste en todas las redes que no son contenidas en ningún área específica, sus enrutadores asociados y los enrutadores que pertenecen a múltiples áreas. El backbone tiene como restricción que debe ser contiguo, lo que lo hace ser el punto de convergencia de todas las áreas del sistema autónomo. Cada una de las interfaces que son configuradas en el área 0 deben ser alcanzables vía otros enrutadores, donde cada interfaz en la trayectoria está configurada como si estuviera en el área 0. A pesar de que el backbone debe ser contiguo, es posible definir áreas en las que ya no lo sea, es decir, donde se rompa la continuidad entre enrutadores. Esto es posible mediante la configuración de *enlaces virtuales*.

### 5.3.3.4 Clasificación de los enrutadores OSPF.

Cuando un sistema autónomo se divide en áreas, los enrutadores pueden clasificarse, de acuerdo a la función que cumplen, en cuatro clases que se traslapan entre sí.

#### Enrutador Interno.

Tiene todas sus interfaces conectadas a redes que pertenecen a la misma área. Los enrutadores con interfaces sólo en el backbone también pertenecen a esta clase. Estos routers ejecutan una sola copia del algoritmo SPF.

#### Enrutador de Borde de Área.

Se unen a múltiples áreas, ejecutan múltiples copias del algoritmo SPF, una por cada área a la que se asocian y una adicional para el backbone. Tienen la misión de condensar la información de sus áreas para su distribución por el backbone, que la distribuye a otras áreas.

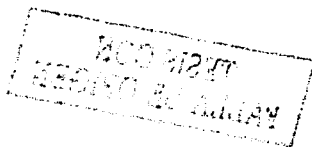
#### Enrutador de Backbone.

Tiene al menos una interfaz conectada al backbone, por lo tanto, incluye también todos los routers que se asocian a más de un área, esto no implica necesariamente que sean routers de borde de área.

#### Enrutador de Borde de AS.

Intercambia información de enrutamiento con otros enrutadores pertenecientes a otros sistemas autónomos. La trayectoria hacia estos routers es conocida por cada uno de los routers del sistema autónomo. Esta clasificación es totalmente independiente de las anteriores, un enrutador de borde de AS puede ser interno o de borde de área, y puede o no participar en el backbone.

La Figura 5.3.3.4 muestra varios tipos de enrutadores OSPF y la relación entre ellos y con todo el ambiente OSPF



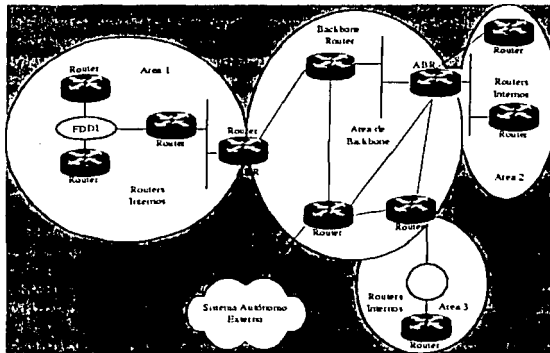


Figura 5.3.3.4. Tipos de enrutadores

### 5.3.3.5 Vecinos y Adyacencias.

OSPF crea adyacencias entre enrutadores vecinos para facilitar el intercambio de información. Los *enrutadores vecinos* son dos enrutadores que tienen interfaces a una red en común. En las redes multiacceso, los vecinos son descubiertos en forma dinámica, utilizando el protocolo de OSPF *Hello*. Una *adyacencia* es una relación formada entre los enrutadores vecinos seleccionados con el propósito de intercambiar información de enrutamiento. No todos los pares de enrutadores vecinos llegan a ser adyacentes. En cambio, las adyacencias son establecidas con un subconjunto de los enrutadores vecinos. Los enrutadores que están conectados por enlaces punto-a-punto o mediante enlaces virtuales son siempre adyacentes. En las redes multiacceso, todos los enrutadores llegan a ser adyacentes el enrutador designado y al enrutador designado de respaldo.

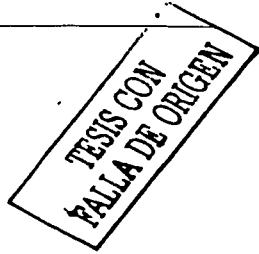
### 5.3.3.6 Enrutador Designado y Enrutador Designado de Respaldo.

Todas las redes multiacceso tiene un router designado y otro que servirá de respaldo en caso de que el primero falle. Las dos funciones principales de este router son:

- Originar los avisos de enlace de red de parte de la red. Este anuncio lista el conjunto de enrutadores, incluyendo el designado, que actualmente están unidos a la red.
- Llegar a ser adyacente a todos los otros enrutadores de la red. Debido a que las bases de datos de estado de enlace son sincronizadas a través de adyacencias (a través de la inicialización de la adyacencia y de un proceso de inundación), el enrutador designado juega un papel principal en el proceso de sincronización.

### 5.3.3.7 Estructura de un paquete OSPF.

TESIS CON  
 FALLA DE ORIGEN



Versión	Tipo	Largo del Paquete
Router ID		
Área ID		
CRC	Tipo de Autentificación	
Autentificación		
Autentificación		
Datos		

Figura 5.3.3.7.1. Estructura de un paquete OSPF

<b>Versión.</b>	1 Byte que identifica la versión del protocolo OSPF utilizada.
<b>Tipo.</b>	1 Byte que identifica el tipo del paquete del OSPF como alguno de los siguientes:  <b>Hello:</b> que establece y mantiene relaciones con los vecinos <b>Descripción de la base de datos:</b> describe el contenido de la base de datos topológica, estos mensajes se intercambian cuando se inicializa una adyacencia. <b>Petición Link-State:</b> solicita a los enrutadores vecinos, una actualización de alguna parte de la base de datos topológica. Estos mensajes se intercambian después de que un enrutador descubre que esas partes de su base de datos topológica no están actualizadas. <b>Actualización Link-State:</b> es la respuesta a un paquete de petición o puede corresponder también a una actualización regular del protocolo de estado de enlace regular, actualizaciones llamadas LSAs. <b>Link-State Acknowledge:</b> paquete de confirmación de las actualizaciones.
<b>Largo del Paquete.</b>	2 Bytes que especifica la longitud del paquete, incluyendo el encabezado OSPF, el valor está medido en bytes.
<b>Router ID.</b>	4 Bytes que identifican el origen del paquete.
<b>Area ID.</b>	4 Bytes que identifican el área a la que pertenece el paquete. Todos los paquetes OSPF están asociados a una sola área.
<b>CRC.</b>	2 Bytes para verificar el contenido total del paquete por si ha sufrido algún daño durante su tránsito.
<b>Tipo de Autentificación.</b>	2 Bytes que contienen el tipo de autentificación, ya que todo el intercambio de protocolos OSPF se autentifica. El tipo de autentificación se configura en cada área.
<b>Autentificación.</b>	8 Bytes que contienen la información de autentificación.
<b>Datos.</b>	Valor variable que contiene información encapsulada de las capas superiores.

#### 4.5 Resumen.

En este capítulo estudiamos las funciones de la capa de red, , además se explico el direccionamiento IP, así como las diferentes clase de redes que existen y las direcciones ip correspondientes a cada clase de red.

---

Por otra parte vimos la finalidad de una máscara de subred, así como la generación de subredes con ejemplos explicados detalladamente.

Por último se vieron los protocolos de enrutamiento más utilizados.

Con esto se finaliza la primera parte de la tesis, con la cual se espera que el lector tenga un panorama profundo de la parte teórica de redes de datos para así poner en práctica estos conocimientos usando el laboratorio propuesto en esta tesis.

---

## **Segunda Parte**

### **Panorama general de la segunda parte.**

En la segunda parte de la tesis se establecen los pasos de diseño y las opciones de implementación apropiadas para el diseño del laboratorio.

El laboratorio no será implementado en el periodo de tiempo en que se desarrolla y termina esta tesis. Debido a esto solo se pueden dar lineamientos generales que serán útiles a la hora de hacerlo, así como ejemplos de implementación diseñados según los lineamientos dados.

Cada tema será abordado primero en la descripción de los aspectos que se consideran como condiciones ideales de diseño, luego se propondrá algún o algunos ejemplos de implementación y también se agregarán sugerencias de implementación.

Al final de la tesis se puede consultar un glosario con los términos más importantes usados a lo largo de esta parte.

---

## Capítulo 6

### 6 Aspectos lógicos y físicos del Laboratorio de Redes. Diseño del laboratorio en condiciones ideales y ejemplos de implementación.

#### 6.1 Introducción.

Las características físicas y arquitectónicas del laboratorio contemplan las dimensiones del mismo, tales como la altura, el área requerida, características del piso, condiciones climáticas, distribución de equipos y de cableado, el cual incluye tanto potencia como datos.

Como ya se ha dicho, primero se dará una visión general de todas aquellas condiciones físicas y lógicas ideales que se recomiendan para un laboratorio de datos como el que se pretende diseñar e implementar, y en particular en este capítulo se enfocará a describir las adecuaciones necesarias que deberán hacerse al lugar destinado para construir un laboratorio de datos.

Los detalles ambientales y arquitectónicos relevantes a considerar en este capítulo para el diseño del lugar, así como el mobiliario que afectará en ello son los siguientes:

- Racks
- Mueblería adicional
- Piso del laboratorio
- Muros y techo
- Iluminación.
- Clima
- Humedad relativa
- Temperatura del laboratorio
- Aire acondicionado
- Requerimientos generales de fuerza.
- Requerimientos de cableado de datos
- Consideraciones generales para la elección del lugar.
- Ubicación de terminales para alumnos.

A continuación se detallará cada uno de estos puntos.

#### 6.2 Racks.

Al tenerse equipos de comunicaciones (DCE's) en el laboratorio, tales como Enrutadores, Fraccionadores, Switches y Hubs, es necesario usar racks o gabinetes para soportar sólidamente y en forma ordenada dichos equipos, minimizando el cableado necesario entre ellos y haciendo más eficiente el espacio ocupado por ellos. Es necesario que dichos equipos estén protegidos ante condiciones ambientales y climáticas adversas, tales como: polvo, humedad, daño malintencionado, accidentes, robo, etc. Para ello es necesario restringir el acceso al laboratorio, o proteger los equipos individualmente cuando éstos se encuentren en un sitio donde el acceso no esté restringido usando gabinetes.

Para el primer caso basta usar racks, con la ventaja de que son más fáciles de instalar y adecuar, además de ser más baratos que los gabinetes.

En la siguiente figura se muestran ambos.

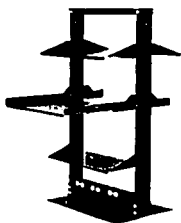


Figura 6.2.1  
Rack industrial de 7 ft de aluminio.



Figura 6.2.2  
Gabinete de 7 ft.

Para el segundo caso, en el que no contamos con un sitio dedicado al laboratorio, es necesario usar gabinetes; los cuales restringen el acceso no autorizado a los equipos, al permitir el acceso al interior del mismo con el uso de una cerradura.

El caso ideal es contar con un lugar dedicado al laboratorio y entonces usar racks para albergar a los equipos.

Adicionalmente a los racks necesarios para instalar los enrutadores, fraccionadores y demás DCE's considerados, se recomienda ampliamente dedicar un rack adicional para conexiones, usando paneles de parcheo con puertos RJ45, BNC y V.35, esto con el fin de concentrar en un solo lugar el cableado proveniente de todos los otros racks y poder interconectarlos fácilmente de acuerdo a las necesidades requeridas. Dicho rack debe tener el espacio necesario para instalar los diferentes paneles de parcheo mencionados anteriormente y mantenerlos ordenados y distribuidos lógicamente dentro del rack, usando etiquetas para identificarlos fácilmente y que, además, se permita un futuro crecimiento en el número de conexiones entre equipos del laboratorio.

Se recomienda que los racks se ubiquen contiguamente uno junto al otro, formando una o dos filas en función del área del laboratorio, y que la distribución permita que se puedan hacer operaciones de configuración, reacondo y de mantenimiento tanto en los equipos como en las escalerillas que albergarán el cableado de datos por un lado y el de fuerza por el otro.

Dado que entre los equipos que se van a instalar en los racks hay enrutadores como los equipos Cisco 7000 y 7010 que tienen dimensiones y peso grandes, los cuales se muestran al final del capítulo, se recomienda usar racks de 7 ft de uso industrial a fin de que soporten adecuadamente el peso de los equipos a instalar en ellos.

Las dimensiones de un rack industrial de 7 pies son las siguientes:

Dimensiones externas:

Altura - 7 ft = 213.4 cm.

Ancho - 19 in = 51.4 cm.

Las dimensiones útiles son menores y deben de tomarse en cuenta en el momento que se haga la distribución de los equipos, ya que algunos equipos pueden requerir de charolas para montarse al rack.

### 6.3 Mueblería adicional para ubicación de equipo didáctico.

Se debe de contemplar la colocación de estantería adicional, esto con el fin de que en dichos muebles se pueda almacenar literatura, manuales, herramientas, cables, equipos en reparación y el material didáctico del que se hablará posteriormente.

El espacio para la mueblería adicional no debe interferir con el área de trabajo destinada a los racks y equipos adicionales, y debe estar ubicada de manera que no interfiera con ninguna de las operaciones habituales del laboratorio.

#### 6.4 Piso del laboratorio

Para el piso del laboratorio se pueden tener dos opciones, una es la de usar un lugar con piso falso y la otra opción es la de tener un lugar sin piso falso.

El piso falso permitiría que el cableado de fuerza y de datos se pueda instalar en forma casi invisible bajo los racks, evitándose el uso de escalerillas en el techo.

Por otro lado si no se tiene piso falso es necesario hacer la canalización por escalerillas en el techo, la cual es más visible y requiere de una altura del techo mayor para permitir la instalación de éstas.

Se debe evitar el polvo y la electricidad estática utilizando piso de concreto, loza o similar y evitar usar alfombra. De ser posible se debe aplicar tratamiento especial a las paredes pisos y cielos para minimizar el polvo y la electricidad estática



Figura 6.4.1 Piso Falso

#### 6.5 Muros y techo.

Es deseable que se considere un lugar que permita tener seguridad ante el acceso a los equipos, y que principalmente los proteja de otros factores tales como son el ambiente, la humedad, el polvo, etc. evitando exponerlos a condiciones y fenómenos que en general perjudican el funcionamiento y seguridad tanto de ellos mismos como de los servicios que proporcionan. El techo puede ser de losa o tener incluso un techo falso de plafón, solo se debe considerar en el momento oportuno, cómo se han que adecuar elementos tales como el cableado, la ventilación, etc. a las condiciones del lugar.

#### 6.6 Iluminación

En cuanto a la iluminación no se requiere que tenga características especiales, simplemente que permita trabajar adecuadamente. Es recomendable que no sea luz natural, ya que si el laboratorio tiene ventanas o tragaluces, se tendría una fuente externa de calor no deseable, lo cual se debe evitar.

Se recomienda que las lámparas del laboratorio sean de luz fría ya que si son una fuente de calor, éste afectara nocivamente la temperatura del lugar.

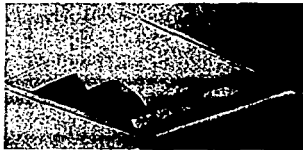


Figura 6.6.1 Lámpara de techo.

TESIS CON  
FALLA DE ORIGEN

#### 6.7 Clima.

Dentro del laboratorio, el clima debe de ser el adecuado para que los equipos trabajen dentro de los límites de operación para los que fueron diseñados, si esto no sucede, los equipos acortan su vida útil y pueden poner en



riesgo no solo la vida del dispositivo y consecuentemente las operaciones y servicios que están destinados a realizar, sino que pueden causar daños o lesiones a los que los operen.

Dentro de las especificaciones de los equipos proporcionadas por los fabricantes se considera que las condiciones óptimas que debe cumplir el laboratorio para que todos los equipos operen correctamente engloban tanto la temperatura como la humedad;

### 6.8 Humedad relativa.

Las condiciones de humedad se requieren sean de entre un 40 % y un 60% de humedad relativa sin condensación. Esto significa que el aire debe estar libre de partículas que puedan condensarse y dañar o corroer los equipos.

### 6.9 Temperatura en el laboratorio.

La temperatura deberá ser la adecuada de acuerdo a las especificaciones de operación de los equipos a fin de que estos no se dañen.

### 6.10 Aire acondicionado.

La manera de controlar la temperatura dentro del laboratorio se sugiere que sea con la ayuda de un sistema de aire acondicionado que regule la temperatura existente en el laboratorio. Esta temperatura interna está en función de factores tales como la temperatura ambiente exterior, la potencia disipada en forma de calor que emiten los equipos al trabajar, el ingreso de luz natural al lugar, etc.

Para ello se deberá elegir un sistema de aire acondicionado de pared o central que renueve el aire que circula en el interior. Para hacer la elección de dicho equipo es necesario tomar en cuenta el volumen total de aire que se debe desalojar en el laboratorio y el tiempo en que lo deba hacer.

### 6.11 Requerimientos generales de fuerza.

Los equipos que se instalarán en el laboratorio necesitan de ciertos requerimientos con respecto a la potencia con la que operarán. Es importante conocer bien los requerimientos de potencia que consumen los equipos operando a su máxima capacidad, esto a fin de que cuando el laboratorio sea operativo, no existan problemas de sobrecarga por consumo excesivo de energía al estar operando todos los equipos.

Los suministros de energía serán a través de corriente directa (-48 V DC), corriente alterna ininterrumpida regulada (127 V AC) y corriente alterna esencial no regulada (127 V AC).

El cableado de fuerza debe ser canalizado utilizando tubería o una escalerilla dedicada exclusivamente al cableado de fuerza. Para el caso de corriente alterna, esta se debe llevar desde los centros de carga ubicados en el mismo laboratorio o en otro lugar, hasta las barras de contactos ubicados preferentemente en la base de cada rack.



Figura 6.11.1 Postes de poder.

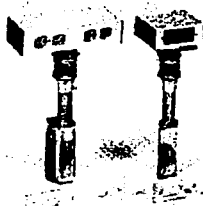


Figura 6.11.2 Potencia sobre piso

Para los tres sistemas de energía citados anteriormente es necesario que cada uno de ellos cuente con un sistema de tierra.

La tierra física se tomará de una cola de tierras ubicada en algún lugar del edificio donde se instalará el laboratorio o una tierra creada ex profeso con una placa de 15 x 30 cm que debe de contar con una impedancia menor o igual a  $5 \Omega$  como requisito de eficiencia.

El cableado de fuerza deberá seguir una trayectoria que permita una adecuada distribución de los contactos en el laboratorio, así como que permita una buena estética.

Esto se puede lograr considerando las siguientes sugerencias:

- Agrupar los cables con cinchos de plástico que sujeten firmemente los mismos a la escalerilla usada para distribuirlos por el laboratorio.
- Es preciso que el cableado siga trayectorias ocultas a fin de que sea lo más estético posible, y además, permita el libre manejo del equipo en caso de que haya necesidad de realizar maniobras con ellos.

En cuanto a centros de carga se debe considerar uno de cada uno de los tres sistemas de energía considerados anteriormente:

- Un centro de carga para CD (-48 V)
- Un centro de carga para AC regulada e ininterrumpida (127 V)
- Un centro de carga para AC esencial (127 V)

La finalidad de solicitar estas tres fuentes de energía es la siguiente:

El circuito de VDC a -48 V se usará para algunos enrutadores y switches principalmente.

El sistema de VAC regulado ininterrumpido se usará para Hubs, Enrutadores, Switches y FCD's.

El sistema de VAC esencial se usará para aquellos dispositivos que no necesiten forzosamente la corriente regulada.

Si no se puede proveer corriente alterna regulada ininterrumpida se deberá proporcionar con un UPS con las características adecuadas para satisfacer la carga requerida por los equipos que lo necesiten y que será conectado a la corriente alterna esencial.

En el caso de que se decida llevar el cableado de fuerza bajo el piso falso, este deberá ser bajado por canaleta o tubería desde el centro de carga correspondiente y llevada a la escalerilla de 6" bajo el piso falso, de donde se distribuirá por debajo de cada uno de los racks y finalmente saldrá por las acometidas para tal fin y llegar a las cajas de contactos en la base de los racks.

En el caso de que se decida llevar el cableado de fuerza por techo, ya sea por que no haya piso falso o por que sea más conveniente, se subirá por canaleta o tubería desde el centro de carga hasta la escalerilla que deberá estar a una altura de 50 cm por arriba de la parte superior de los racks, y luego distribuida por encima de todos los racks en donde bajara el cableado necesario para cada uno de ellos hasta las cajas de contactos en la base de cada rack y en los lugares que sea necesaria una toma adicional para usos futuros.

Para ello es necesario considerar si en el lugar hay o no plafón o techo falso ya que de ser así la canalización se deberá hacer por arriba del mismo para evitar que sea visible.



Figura 6.11.3 Diferentes tipos de canaletas.

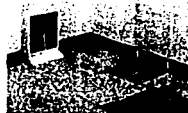


Figura 6.11.4 Ductos de pared.

---

Cada centro de carga deberá tener una etiqueta al frente en un lugar siempre visible, que indique el tipo de corriente que maneja. Se sugiere que el cableado tenga el siguiente código de colores a fin de identificarlo con facilidad cuando sea necesario.

- Corriente directa: negativo (rojo), positivo (negro) y tierra física (verde)
- Corriente alterna esencial: fase (negro o gris claro), neutro (blanco) y tierra física (verde)
- Corriente alterna regulada ininterrumpida: fase (negro o gris claro), neutro (blanco) y tierra física (verde)

#### **6.12 Requerimientos de cableado de datos.**

El cableado de datos se hará concentrando el cableado proveniente de los racks con equipos, hacia el rack que se dedicará exclusivamente a paneles de parcheo, se recomienda que si se tiene una distribución de los racks en filas, el primer rack sea el dedicado para paneles de parcheo, esto es con el fin que cuando haya crecimientos del laboratorio en el futuro se puedan agregar a la fila estos nuevos racks en forma consecutiva con los otros.

Para el cableado entre el rack de parcheo y los otros racks se usaran diversos tipos de cable, entre los cuales estará cable coaxial, cable UTP categoría 5, y cable V.35.

Cada uno de estos tipos de cable llegara a un panel de parcheo adecuado, y lo hará por una escalerilla dedicada exclusivamente a datos.

Para tener de manera ordenada y controlada este cableado se requiere que se use un sistema de etiquetas que evite confusiones con la manera en que está distribuido dicho cable. Sobre la escalerilla se requiere que se sujete el cableado con cinchos de plástico para evitar que se mueva y para poder agrupar cables de diferentes tipos o diferentes racks.

En el capítulo correspondiente se detallarán a fondo la manera en que se realizará el cableado y el etiquetado del mismo. Asimismo la distribución del cableado se describirá posteriormente.

#### **6.13 Dimensionamiento físico del laboratorio.**

Se deben considerar para el dimensionamiento global del laboratorio, las especificaciones generales del lugar en donde éste se instalará, ya que de ello dependen en gran medida las variantes de diseño y uso de los recursos con los que se dispongan.

Bajo estos lineamientos se detallan los puntos a tratar con respecto al dimensionamiento del laboratorio en condiciones ideales.

Se debe de considerar la distribución de espacios a fin de poder conocer finalmente las dimensiones requeridas para el lugar, para ello se deben hacer las siguientes consideraciones:

¿Qué equipos se usarán?

¿Qué tipo de racks se usarán?

¿Qué centros de carga se usarán?

¿Qué equipo de aire acondicionado se usará?

¿Qué espacio es necesario para el trabajo de usuarios? y

¿Qué mueblería se requiere instalar y considerar para la óptima operación del laboratorio?.

Entre todas estas consideraciones que se deben contemplar para el dimensionamiento del laboratorio están las siguientes:

- Espacio para racks.  
Se deben tener en cuenta las características de los racks ya que ocuparán un lugar importante en el laboratorio, estos deben de poder ser instalados con comodidad y considerar el espacio necesario para poder instalar en ellos los equipos y servicios del laboratorio.
- Espacio entre racks.

---

Este es el espacio necesario para evitar que los racks estén demasiado pegados, lo cual ocasionaría dificultad para la instalación de los mismos y los servicios necesarios, además de que dificultaría poder tender el cableado y hacer el mantenimiento del mismo.

- **Espacio para mueblería adicional.**

Este espacio es requerido para tener los muebles necesarios para guardar el material didáctico, herramientas y equipo adicional que se tuviera.

- **Espacio para las terminales de alumnos y profesor.**

Este espacio es necesario para poder ubicar las terminales con las que se trabajará en el laboratorio. Es decir el espacio para sillas y muebles individuales o mesas donde colocar dichos equipos.

- **Espacio para crecimiento.**

Se debe considerar y reservar espacio para crecimientos futuros, ya que el laboratorio en algún momento requerirá ampliarse con más racks y equipos, por lo que se debe visualizar y evitar que a futuro se tenga que modificar drásticamente el diseño inicial del laboratorio

Como conclusión, las dimensiones totales del laboratorio deben de contemplar la asignación del espacio necesario para cada uno de los puntos mencionados anteriormente, más el espacio reservado para crecimiento futuro.

#### **6.14 Ubicación de terminales para alumnos.**

Para acceder a los equipos del laboratorio, para hacer configuración o pruebas es necesario contar con terminales conectadas a los equipos. Para esto se tienen dos alternativas. De estas dos alternativas se debe elegir una, y debe de tenerse en cuenta para el diseño inicial:

- El área de trabajo de los usuarios locales estará en el mismo lugar que se encuentre físicamente el laboratorio.
- El área de trabajo de los usuarios locales estará en un lugar distinto al sitio donde esté físicamente el laboratorio.

Las terminales para los alumnos independientemente donde sean ubicadas, requerirán espacio para ser instaladas, además de los servicios necesarios para poder trabajar con ellas, como son potencia, cableado de datos, mueblería, etc.

Ambas alternativas sugieren dos enfoques para el diseño del área del laboratorio:

##### **Primera opción:**

Los usuarios coexisten físicamente con los equipos, implica pensar desde el principio en que el lugar tendrá que contar con un espacio adecuado para que puedan trabajar sin problemas tanto los equipos como los usuarios.

Esto significa que también se deberán tomar en cuenta para el desarrollo de las prácticas, el que los usuarios tengan la libertad de poder interactuar con los equipos directamente, cuando sea necesario o recomendable.

Un sitio que concierte tanto a los equipos y usuarios necesita ser de mayores dimensiones y para planearse se deben incluir aspectos tales como una distribución adecuada de equipos, cableado apropiado que permita a los usuarios trabajar en forma adecuada, espacio adicional para los equipos desde los cuales se pueda acceder a los equipos de comunicaciones, espacio para gavetas o estantes donde se coloquen materiales, literatura y accesorios adicionales para el desarrollo de las prácticas y labores de operación y mantenimiento.

##### **Segunda opción:**

Los usuarios están en un lugar diferente a donde se encuentra el laboratorio y, por tanto, solo puedan acceder al mismo por vía remota, implica que se tengan que planear dos salas diferentes, una desde la cual se acceda a los equipos y aquella donde se encuentren los mismos, aunque esta última no requiere demasiado, ya que

desde un equipo con acceso a nuestra red bastaría. En cuanto a la segunda solo se pueden dar lineamientos generales de qué es lo que se recomienda, los cuales se darán mas adelante en esta tesis. Por otro lado, al carecer los usuarios del contacto directo con los equipos, no se podrán incluir en las prácticas temas o tópicos en los que se requieran de estas libertades.

### **6.15 Ejemplo de distribución de espacios.**

Las condiciones descritas anteriormente respecto a las condiciones físicas son las recomendadas, y dado que no es posible implementar el laboratorio de inmediato, solo quedan como lineamientos generales que hay que seguir lo mejor posible, quedando claro que dichas condiciones se deberán adecuar también a los recursos disponibles al momento de la implementación, los cuales no se conocen aún. Si se cuenta con los recursos suficientes se debe de implementar lo más próximo posible a lo ideal, pero si los recursos son escasos se debe de suprimir algunas detalles por otros más importantes.

Los aspectos que se deben resolver o modificar hasta el momento de la implementación, dado que dependen de las condiciones del lugar elegido son los siguientes:

- **Piso del laboratorio.**

La consideración del tipo de piso del laboratorio es muy importante para poder definir la estrategia a seguir para realizar la implementación física del laboratorio, ya que definiera si se usa piso falso, escalerillas, tubería o canaleta para realizar las labores de empotrado del rack, cableado de datos y potencia. En el capítulo correspondiente se detallan las diversas opciones que se pueden tener.

- **Muros y techo.**

Este aspecto no es tan impactante en la implementación del laboratorio, simplemente con que cumpla con las especificaciones mínimas de protección señaladas anteriormente será suficiente.

- **Iluminación**

Si las condiciones de luz del lugar elegido lo ameritan será necesario instalar iluminación adecuada. Sin embargo eso corresponderá a terceros que deberán seguir las recomendaciones dadas al hacerlo.

- **Clima.**

Como ya se dijo, si el clima no es apropiado para albergar los equipos será necesario instalar clima artificial a fin de adecuar el sitio.

- **Mueblería adicional para ubicación de equipo didáctico adicional.**

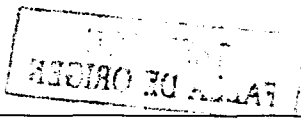
La mueblería será proporcionada por la Facultad de Ingeniería. El proceso y tiempos de adquisición están fuera de nuestro alcance.

Sin embargo las características de los muebles no están sujetas a condiciones de elección tan severas y será fácil adecuarse a los que puedan ser proporcionados.

- **Temperatura.**

Según las especificaciones de los equipos, el rango de temperatura dentro del laboratorio se deberá encontrar entre 18 a 25 grados centígrados y debe haber una variación de temperatura menor o igual a 3 grados C/hora.

Un ejemplo de cómo se visualiza que deba quedar el laboratorio con respecto al dimensionamiento físico y la ubicación de terminales para alumnos y racks es mostrado en la siguiente figura:



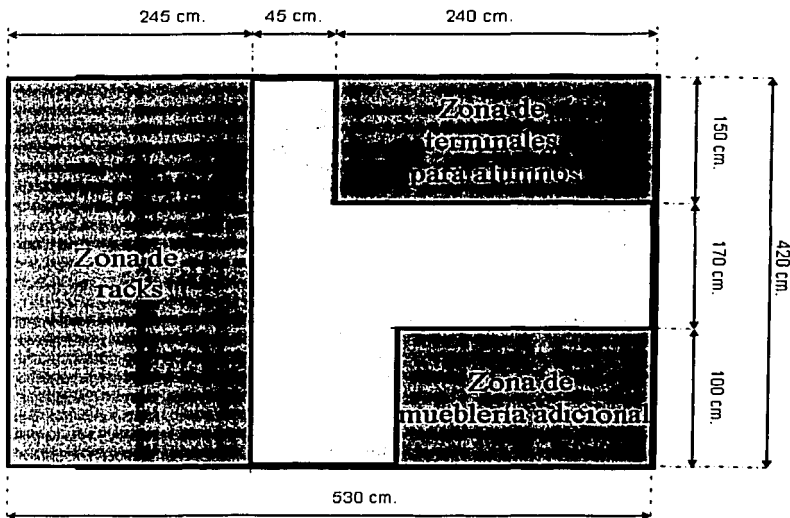


Figura 6.15.1 Distribución de espacios sugerida para el laboratorio.

Se pueden hacer las siguientes observaciones de la figura anterior:

Las medidas mostradas son las mínimas requeridas, de acuerdo a las dimensiones reales de los racks y equipos a usar.

La zona de terminales de alumnos tiene el espacio aproximado para colocar 3 o 4 terminales o estaciones de trabajo, que son suficientes para poder albergar a un grupo pequeño de usuarios, así como los muebles que son necesarios para tal fin. Esto suponiendo que las terminales de alumnos se encuentren en la misma habitación, de no ser así, se deben de tomar las medidas apropiadas.

Como se dijo se pueden tener las opciones de tener terminales de usuarios en el sitio o remotamente, en este momento, la decisión de dónde se ubicarán las terminales de los alumnos, no es tan relevante y se definirá en el momento de implementación, considerando ya los aspectos técnicos, de operación y los recursos disponibles con los que se cuenta.

La zona de racks señalada se visualiza con la distribución de racks mostrada en la siguiente figura:

TESIS CON  
FALLA DE ORIGEN

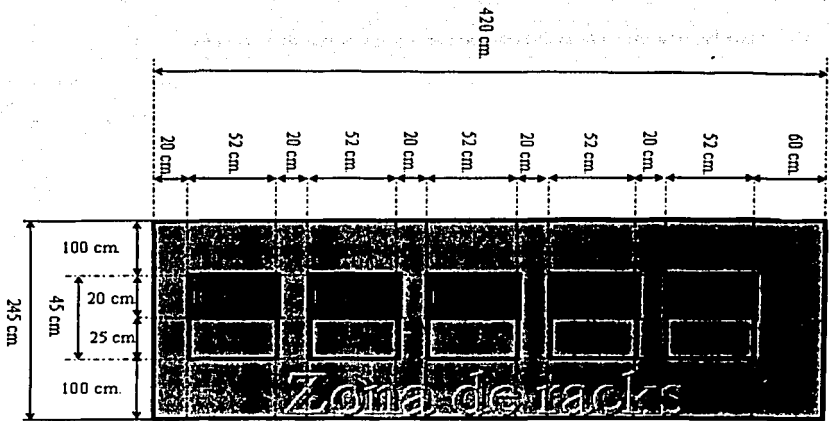


Figura 6.15.2 Distribución sugerida de racks (En la zona de racks.)

La figura muestra la distribución que deben de tener los racks y las medidas mínimas que deben de tener con respecto al espaciamiento entre ellos. Si es necesario deben de agregarse líneas de racks paralelas a la primera, para crecimiento futuro.

El espacio en gris junto al rack es el espacio que ocuparán los equipos más grandes.

También se deben de manejar el espacio necesario para poder hacer maniobras en el rack y los cables que salen de ellos.

El espacio entre racks debe de permitir el poder colocar guarda cables y hacer maniobras, por eso se deja un espacio grande para ello.

El rack 0 se utilizará como rack de paneles de parcheo. En el capítulo siguiente se explicará la manera en que se distribuirán los equipos dentro de los racks.

### 6.16 Resumen.

Este capítulo trata de dar los lineamientos generales para calcular la distribución de espacios en el laboratorio, tomando en cuenta todos los aspectos posibles.

Se debe recalcar que los lineamientos ideales para la construcción del laboratorio de datos, deben tratar de seguirse lo mejor posible, ya que lo que persiguen es hacerlo completamente operacional, seguro y eficiente.

Finalmente se debe tener conciencia de que una vez que se cuente con los recursos finales, será necesario adecuarlos y administrarlos de la mejor manera para poder adaptarse a las carencias que se puedan tener, siempre tratando de optimizar dichos recursos.

TESIS CON  
FALLA DE ORIGEN

---

## Capítulo 7

### 7 Recomendaciones para la instalación de equipos dentro de los racks.

#### 7.1 Introducción.

En este capítulo se dan los lineamientos generales a seguir, para la distribución e instalación de los equipos dentro de los racks que serán colocados dentro del laboratorio, y que servirán para albergar a los equipos con los que cuente el mismo.

Hay varias razones por las cuales es importante planear con cuidado la manera en que los equipos se distribuyen en los racks, ya que tiene consecuencias directas en el futuro, como la manera en que se podrá trabajar con los equipos una vez que el laboratorio se haga operacional.

Se necesitará flexibilidad para hacer cambios en la conexión de los equipos durante el desarrollo de las prácticas a realizarse en el laboratorio, ya que se necesitará poder hacer diversas configuraciones y topologías físicas y lógicas en la conectividad de los equipos usados.

Los equipos una vez instalados no serán movidos, y entonces todos los cambios en la configuración de la conexión serán hechos usando puentes en los paneles de parcheo, ya sea en el mismo rack donde estén los equipos para el caso de conexiones entre los equipos de un solo rack o en el rack dedicado a parcheo cuando se trate de configuraciones en que se requieran interconectar equipos en más de un rack. Esto último se debe tener en cuenta al momento de decidir cuales equipos se repartirán en los racks.

Los puntos a considerar antes de la asignación definitiva de los equipos en cada uno de los racks son los siguientes:

- Distribución y separación mínima entre equipos dentro del rack.
- Distribución de fuerza por rack y aterrizado eléctrico de equipos.

#### 7.2 Distribución de equipos en racks.

Los equipos se instalarán en racks de uso industrial de 7 pies, dichos racks tienen la suficiente robustez para soportar los equipos que se instalarán en los mismos.

Las dimensiones de un rack industrial de 7 pies son las siguientes:

Dimensiones externas

Altura 7 ft = 213.4 cm.

Ancho 19 in = 51.4 cm.

Las dimensiones útiles son menores a las externas, y deben de tomarse en cuenta en el momento que se haga la distribución de los equipos ya que algunos pueden requerir de charolas.

Para hacer la asignación y distribución de espacios en el espacio útil dentro de los racks, es necesario considerar:

- Las dimensiones de cada uno de los equipos a ser montados en los racks.
- La cantidad de equipos con los que se contará y se instalarán en el laboratorio a fin de poder saber cuantos racks serán necesarios en el laboratorio.
- Considerar el espacio reservado para futuros crecimientos.
- Que topología o topologías de conexión de los equipos se pretenden usar en las prácticas.
- El uso o función principal que se le va a dar a cada rack.

Para la consideración del primer punto es necesario conocer las especificaciones provistas por el fabricante de los equipos a instalar. En este caso se requieren conocer las dimensiones exteriores máximas de los equipos



---

en sus tres dimensiones (altura, ancho y profundidad), esto es, las dimensiones que el equipo ocupará una vez que se haya instalado con todos sus accesorios y dispositivos externos, tales como fuentes de poder, tarjetas, cables, etc.

La cantidad de equipos que se instalarán es necesario conocerlo ya que solo así es posible determinar cuantos equipos y de que tipo irán en cada rack, así como saber la cantidad total de racks que se necesitarán en el laboratorio.

En general se puede adelantar que lo ideal sería tener racks con equipos muy similares, a fin de que se puedan tener equipos de diferentes capacidades en cada uno, de que el peso en los racks se soporte de manera adecuada y para permitir realizar conexiones físicas en diferentes tipos.

En el diseño de una red de datos se debe de tener siempre en cuenta que la red que se diseñe, seguramente en un futuro a mediano o largo plazo, sufrirá de cambios en su estructura y tamaño, estos cambios en general, serán en el sentido de un crecimiento para incrementar su capacidad, así que en este caso, es necesario que en un buen diseño del laboratorio se consideren dichos cambios a futuro.

En el caso del laboratorio, este crecimiento se considera principalmente en la reservación de lugar para la adición de nuevos racks, así como una instalación eléctrica con capacidad extra a la requerida.

El rack de parcheo concentrará el cableado proveniente de los otros racks, y por tanto tendrá paneles de parcheo para RJ45, V.35 y BNC, así como un enrutador que se dedicará para el acceso a Internet y algún equipo adicional.

Los paneles de parcheo para RJ45 se situarán en la parte superior del rack, siguiendo un etiquetado de izquierda a derecha y de arriba hacia abajo, los paneles de parcheo para BNC se situarán en la parte inferior del rack, siguiendo un orden de numeración y etiquetado de abajo hacia arriba y de derecha a izquierda y los paneles de V.35 se colocaran en la parte media del rack siguiendo un orden de numeración de arriba a abajo y de izquierda a derecha.

Esto es con el fin de reservar un espacio para crecimientos futuros, en que se requieran probablemente más paneles para recibir a más racks.

En el centro del rack se colocara un enrutador que será dedicado al enlace que conectará a Internet al laboratorio.

Dicho enrutador será la salida de datos del laboratorio y por esto se colocará en el rack de parcheo.

Como previsión en el caso de crecimiento futuro, se debe dejar espacio libre para poder colocar mas paneles de parcheo provenientes de los racks adicionales.

La separación mínima entre equipos en general debe de seguir los lineamientos siguientes:

A partir de la base del rack se deben dejar 20 cm desocupados antes de poner el primer equipo, que en general es el más pesado.

Después de ello se deben dejar 5 o 10 cm entre equipo y equipo, con el fin de que éstos no estén en contacto directo.

Sabiendo cuales equipos irán en cada rack, estos se distribuyen de abajo hacia arriba, colocando los de mayor peso en la parte inferior.

Una vez que están colocados los enrutadores, se deben instalar sobre éstos los paneles de parcheo, cuidando de dejar un espacio de 20 cm medidos desde la parte superior a fin de prever un crecimiento futuro.

Las instrucciones y pasos a seguir para poder instalar los equipos son especificados por el fabricante, así como los kits de instalación para facilitar esa tarea, dicho proceso dependerá de las dimensiones físicas de los aparatos y de los cuidados y pasos que requieran para su correcta instalación

En cuanto al rack dedicado a parcheo, la separación entre paneles de parcheo no es necesaria, es decir que los paneles pueden estar contiguos unos a los otros.

### 7.3 Distribución de la potencia de fuerza en los racks.

La potencia requerida en cada rack depende directamente de cuantos y qué tipo de equipos estén instalados en él, por lo que se deberá hacer el cálculo de cuanta potencia o amperaje requiere cada equipo en el rack, y después de sumar esas corrientes o potencias, poder determinar cuanta energía es la que se necesita en cada rack.

Las especificaciones de energía consumida por cada equipo son proporcionadas por el fabricante del mismo, generalmente en sus hojas técnicas, por lo que es necesario obtenerlas para poder tener esa información, asimismo influye si el equipo tiene instaladas tarjetas adicionales o fuentes extras que incrementan el consumo de energía.

Se debe de proveer a los equipos con la energía necesaria para su correcto funcionamiento, ya que si la demanda de energía de los equipos es mayor a la suministrada, las consecuencias podrían llegar a ser hasta el daño físico de los equipos y de la instalación eléctrica.

En cuanto a los sistemas de energía necesarios para que trabajen los equipos, es muy importante tenerlos bien aterrizados, ya que si esto no es así se puede tener un riesgo mayor, de que una descarga, un cortocircuito o un accidente en el sistema eléctrico, haga que los equipos se puedan dañar, lo cual es necesario evitar a toda costa.

### 7.4 Ejemplo de implementación.

La distribución de equipos en los racks depende obviamente de los equipos con los que se cuente, y dado que no sabemos aun con certeza los equipos de los que dispondremos solamente es posible dar un ejemplo de la distribución de equipos en los racks. Para ello se deben seguir las especificaciones dadas en este capítulo.

Los equipos considerados para la implementación del laboratorio no se conocen con precisión, pero se espera que sean los siguientes, entre ellos hay enrutadores Cisco de las series 7000, 4000 y 3000 así como fraccionadores RAD.

La siguiente tabla contiene una lista tentativa de los equipos con los que se espera contar.

Cantidad	Descripción del equipo.
10	Fraccionador RAD Mod. FCD-2
1	Switch WS-C1400(CDDI/FDDI)
1	Bridge STS-10x
5	Access Server Cisco 500-CS
2	Bridge Cisco WS-C1201
3	Enrutador Cisco AGS+
12	Enrutador Cisco 3000
5	Enrutador Cisco 4000
5	Enrutadores Cisco 7000

Tabla 7.4.1 Equipos tentativos para el laboratorio.

Las dimensiones de estos equipos según las especificaciones del fabricante son las siguientes:

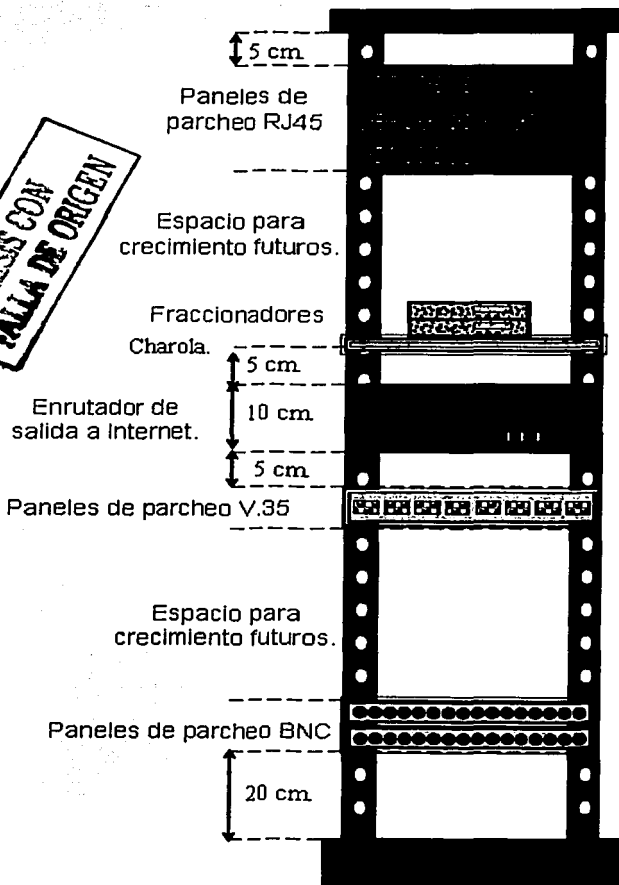
Equipo	Peso	Dimensiones (cm.).		
		Altura	Ancho	Profundidad
Enrutador Cisco 3000.	6.8 Kg.	10 cm.	33 cm.	35.6 cm.
Enrutador Cisco 4000.	10.9 Kg.	8.6 cm.	44.7 cm.	45 cm.
Enrutador Cisco 7000 con tarjetas y fuentes.	65.7 Kg.	48.9 cm.	44.45 cm.	63.75 cm.

Enrutador Cisco AGS+.	25.45 Kg.	25.4 cm.	44.45 cm.	50.8 cm.
Bridge Cisco WS-C1201	7.7 Kg.	6.96 cm.	44.2 cm.	40.6 cm.
Access Server Cisco 500-CS	2.27 Kg.	6.3 cm.	36.8 cm.	27.9 cm.
Switch Cisco WS-C1400	7.3 Kg.	6.86 cm.	45.72 cm.	40.64 cm.
Fraccionadores RAD.	3 Kg.	5 cm.	30 cm.	30 cm.

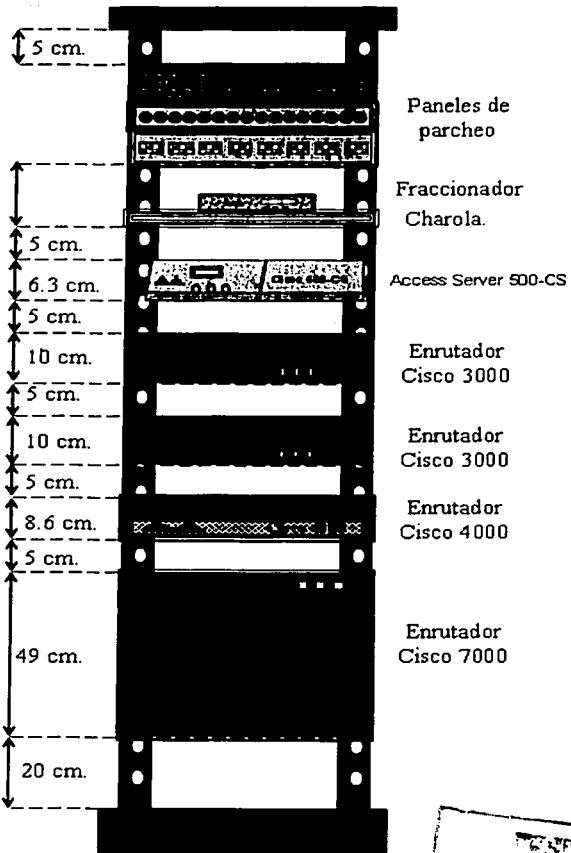
En base a estas dimensiones se define el espacio ocupado por los equipos una vez instalados en el rack, a fin de que permitan el trabajo cómodo y seguro cerca de ellos.

Un ejemplo de cómo se visualiza que deben quedar los equipos en los racks de acuerdo a las especificaciones dadas es mostrado en las siguientes figuras:

**TESIS CON  
PALLA DE ORIGEN**

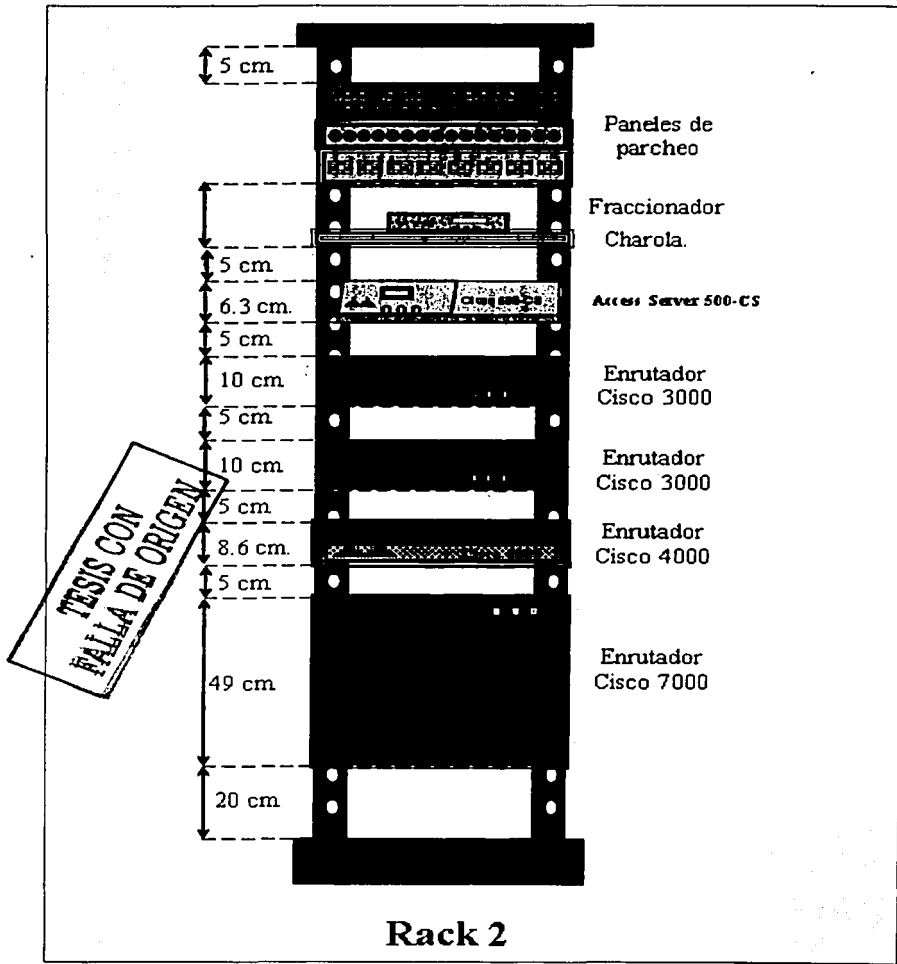


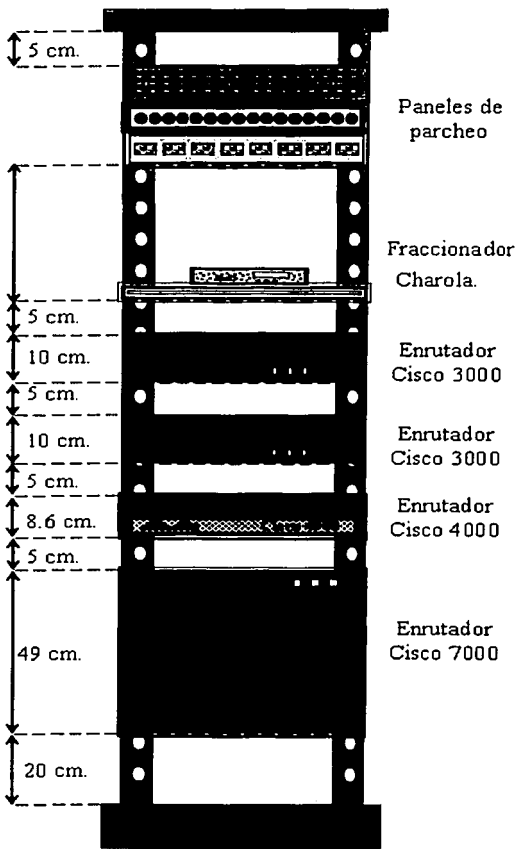
**Rack 0**



**Rack 1**

TESIS CON  
SALA DE ORIGEN

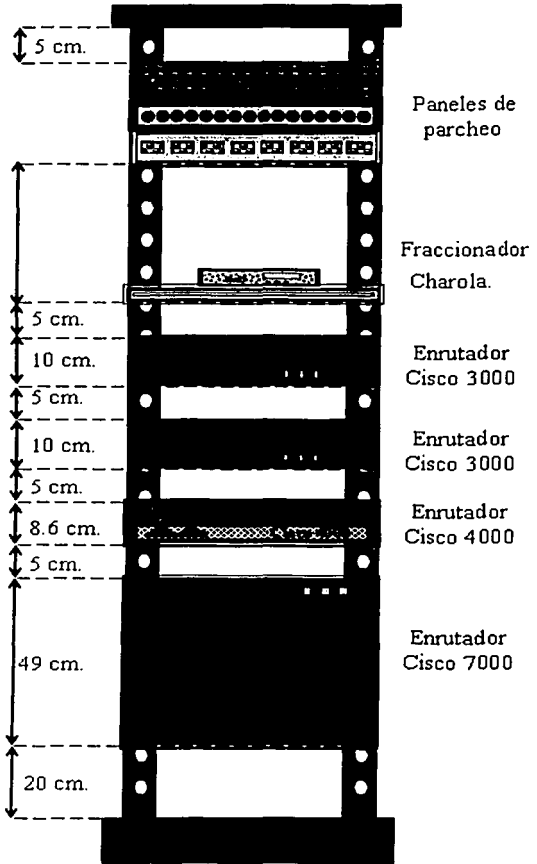




**Rack 3**

TESIS CON  
FALLA DE ORIGEN

TESIS CON  
FALLA DE ORIGEN

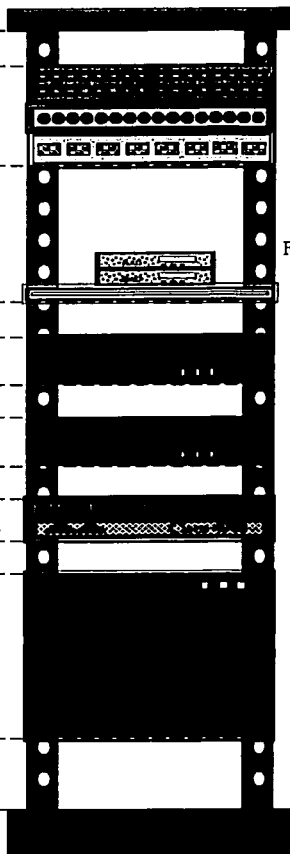


**Rack 4**



5 cm.

5 cm.  
10 cm.  
5 cm.  
10 cm.  
5 cm.  
8.6 cm.  
5 cm.  
49 cm.  
20 cm.



Paneles de parcheo

Fraccionadores

Charola.

Enrutador  
Cisco 3000

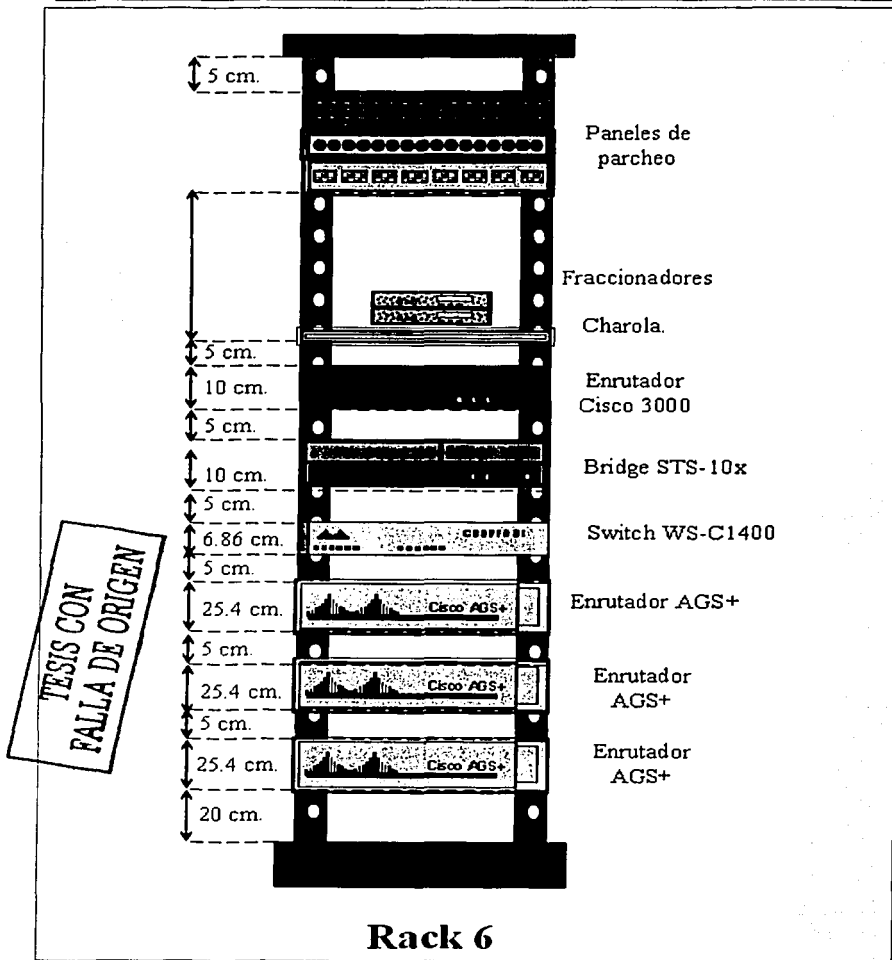
Enrutador  
Cisco 3000

Enrutador  
Cisco 4000

Enrutador  
Cisco 7000

## Rack 5

TESIS CON  
FALLA DE ORIGEN



## Rack 6

Figura 7.4.1 Distribución sugerida de equipos en cada uno de los racks.

---

En las figuras se muestran todos los racks y equipos con los que se planea contar.

En el primer rack, dedicado a paneles de parcheo, se muestra como se distribuyen los patch paneles RJ45, BNC, V.35 y el enrutador que se dedicará a la salida a Internet.

El resto de los racks es en donde se albergaran los equipos. En estos se colocan diversos tipos de enrutadores tratando de que en cada uno haya por lo menos un enrutador de cada tipo.

Los fraccionadores y otros equipos de pequeñas dimensiones serán colocados en charolas en la parte superior de los racks, esto debido a sus dimensiones y poco peso.

Las charolas pueden ser adquiridas en varios tamaños de acuerdo al equipo que pueden contener, por lo que será necesario revisar las diferentes opciones disponibles.

El espacio mostrado entre equipo y equipo es el sugerido a fin de evitar que no estorben al trabajar con ellos y permitir que operen correctamente.

Las dimensiones mostradas no están en las proporciones exactas.

En lo que se refiere al panel de parcheo, se colocaron los paneles tal como se describió en puntos anteriores, organizando los paneles de acuerdo a su uso e importancia y considerando espacio para crecimientos futuros. La manera en que se rematan los cables en los paneles de parcheo, así como la cantidad de cables que se deberán tender entre rack se describe en el capítulo dedicado al cableado.

## **7.5 Resumen.**

En este capítulo se dieron los lineamientos y consideraciones generales a seguir en la instalación de los equipos dentro de los racks, tanto en los detalles a considerar para hacer la decisión de cómo repartirlos en los mismos, como aquellos a seguir para instalarlos adecuadamente. Así mismo se mostró un ejemplo de cómo se visualiza que queden los racks y los equipos.

Sin embargo estos lineamientos son solo una guía para el momento en que se realice la implementación final del laboratorio, hasta ese momento, se tomarán en cuenta los recursos disponibles con los que se cuente para el laboratorio y las limitaciones técnicas.

---

## Capítulo 8

### 8 Cableado para la interconexión de equipo.

#### 8.1 Introducción.

El cableado para la interconexión del equipo es un elemento básico para el diseño del laboratorio, la adecuada planeación del cableado estructurado nos dará flexibilidad para el uso de los equipos instalados. Se considera necesaria la concentración del cableado en un solo lugar de tal forma que sea posible disponer a través de él, de conexiones a los equipos distribuidos en todo el laboratorio. El lugar de concentración será el rack número cero, dedicado exclusivamente para paneles de parcheo y descrito en el capítulo anterior.

En este rack dedicado a paneles de parcheo, se podrán realizar con orden y facilidad, las conexiones entre los equipos instalados en los demás racks a través de puentes hechos con cables de corta longitud. Además de ser fácil de realizarse, nos permite hacer múltiples configuraciones de conexión entre los equipos que se necesiten, sin el problema de realizar cambios en el cableado.

Al momento de establecer la ruta del cableado es una consideración primordial evitar el paso del cable por los siguientes dispositivos:

- Motores eléctricos grandes o transformadores (mínimo 1.2 metros.)
- Cables de corriente alterna.
  - Mínimo 13 cm. para cables con 2KVA o menos.
  - Mínimo 30 cm. para cables de 2KVA a 5KVA.
  - Mínimo 91 cm. para cables con más de 5KVA.
- Luces fluorescentes y balastos (mínimo 12 centímetros.)
  - El ducto debe ir perpendicular a las luces fluorescentes y cables o ductos eléctricos.
- Intercomunicadores (mínimo 12 cm.)
- Equipo de soldadura.
- Aires acondicionados, ventiladores, calentadores (mínimo 1.2 metros.)
- Otras fuentes de interferencia electromagnética y de radio frecuencia.

Esto es con el fin de evitar la Interferencia electromagnética que es perjudicial a la comunicación de los datos a través del cableado de datos y al sistema de potencia del laboratorio.

#### 8.2 Cableado Intrarrack.

El cableado intrarrack es aquel cableado que se encuentra distribuido entre los equipos de un solo rack, y que concentra en un panel de parcheo las conexiones a cada dispositivo en el mismo, para ello se necesitan diferentes tipos de cables y de interfaces, tales como: RJ45, el coaxial y el V.35

Estos paneles de parcheo nos permitirán realizar conexiones entre equipos del mismo rack, sin necesidad de hacerlo hasta el rack de paneles de parcheo, y además permitirá que se pueda realizar en cada rack una configuración similar o diferente de los equipos instalados en él, según convenga, dependiendo de cuál sea la necesidad para cada práctica que se realice.

#### 8.3 Cableado Interrack.

El cableado interrack concentra el cableado proveniente de los paneles de parcheo de cada rack, el cual a su vez concentra el cableado intrarrack y lo lleva al rack dedicado a paneles de parcheo, por lo tanto es necesario que dicho cableado sea de las mismas características y tenga las mismas interfaces que se usan en el cableado intrarrack.

Además del cableado necesario para concentrar el proveniente de cada uno de los racks existentes se debe contemplar espacio adicional para instalar más cableado como previsión de un futuro crecimiento en el que se necesiten instalar más racks o equipos en el laboratorio.

El cableado debe de ser lo más funcional y estético posible, de manera que el cableado no estorbe de ninguna manera, ya sea para realizar mantenimiento o cambios en la distribución del mismo.

---

También debe considerarse que cada tipo de panel de parcheo tiene una ubicación definida en cada rack, lo cual ya fue tratado en el capítulo anterior.

En este tipo de cableado es necesario usar escalerillas, ductos o canaleta tal como se describió en capítulos anteriores

Y como se dijo, la elección de estos esta en función de las características físicas y arquitectónicas del lugar.

A continuación se describe cada uno de los tipos de cableado necesarios para la interconexión de los equipos en los racks. Cada tipo de panel de parcheo puede tener en el otro extremo de los cables conectados, otro panel de parcheo de iguales características o puntas rematadas con el mismo tipo de conector usado, aunque si es necesario, se pueden hacer conversiones de conectores usando "transceivers".

#### **8.4 Panel de parcheo RJ45.**

El panel de parcheo de RJ45 se necesita para conectar aquellos equipos que utilicen cable UTP de diversas categorías y conectores de tal tipo, los cuales son ocupados por diferentes tecnologías de red. La más sobresaliente y común es Ethernet, aunque hay otras.

La cantidad de puertos requeridos en el panel de parcheo RJ45 se dejará por el momento pendiente, ya que será definido cuando se haya decidido la distribución final de los equipos en cada rack, y por tanto la necesidad de cierta cantidad de este tipo de puertos que deban existir para conectar los equipos instalados. Pero se debe prever que la cantidad de este tipo de puertos es mayor que la de los otros tipos.

La cantidad de puertos que tienen los diferentes paneles de parcheo existentes en el mercado varía, ya que existen con 12, 24, 48 o 96 puertos. Esto quiere decir que se podrían concentrar en un solo panel de parcheo tanto el cableado interrack como el intrarack.

La manera en que se rematan los cables en el panel de parcheo se describe más adelante.

#### **8.5 Panel de parcheo V.35.**

El panel de parcheo V.35 se necesita para conectar aquellos equipos, que utilicen conectores de este tipo para terminar el cable serial, lo que incluye a la mayoría de los enrutadores.

La cantidad de puertos necesarios en el panel de parcheo V.35 se dejará por el momento pendiente, ya que será definido cuando se haya decidido la distribución final de los equipos en cada rack y por tanto la necesidad de cierto número de este tipo de puertos que tengan que existir para conectar los equipos instalados.

La cantidad de puertos que tienen los diferentes paneles de parcheo V.35 existentes en el mercado es menor que los que tienen los de puertos RJ45, ya que los V.35 tiene 8 puertos, ya que son de mayores dimensiones que los anteriores.

La manera en que se rematan los cables en el panel de parcheo se describe más adelante.

#### **8.6 Panel de parcheo BNC.**

El panel de parcheo de BNC se necesita para conectar aquellos equipos que tengan puertos que utilicen conectores de tal tipo para rematar cable coaxial.

Se colocan los paneles de parcheo BNC necesarios en cada rack, de manera que pueda hacerse el cableado Interrack y el Intrarack. El número de puertos BNC en paneles de parcheo comerciales es variado, ya que dependiendo del panel de parcheo seleccionado, éste puede tener 16, 32 o más puertos.

La manera en que se rematan los cables en el panel de parcheo se describe más adelante.

#### **8.7 Arreglo del cableado fijo dentro y fuera del rack.**

El cableado una vez rematado en los paneles deberá ser acomodado de tal manera que éste no sea visible, esto a fin de tener una instalación limpia y estética, además, el cableado deberá ser agrupado de acuerdo al tipo de cable y sujeto al rack con cinchos de plástico o cordones para que no se mueva fácilmente. Es decir el cable UTP no deberá ir sujeto junto con el coaxial y lo mismo para los otros cables.

Para el cableado interrack se recomienda usar escalerillas, canaletas y usar guardas para bajar o subir el cable por los costados del rack, tal como se mencionó en capítulos anteriores.

### 8.8 Etiquetado

El etiquetado es necesario para poder identificar con facilidad el cableado instalado, además de que permite un más fácil y mejor mantenimiento del mismo. Se considera además una buena costumbre que se documente la manera en que se distribuye el cableado tanto dentro como fuera del rack y numerarlo metódicamente para su fácil identificación.

### 8.9 Elaboración del cableado

A continuación se describirá la manera en que se elaboran los diferentes tipos de cableado.

#### 8.9.1 Cableado UTP.

El tipo de cableado con el que más se va a trabajar es el UTP; con él se van a elaborar los patch cords para Ethernet y para las conexiones a las consolas de los equipos.

Existen varias categorías de cable UTP, la diferencia entre ellas es la frecuencia máxima de operación que pueden soportar, a continuación se da una lista de las principales categorías de cable UTP

Categoría	Frecuencia de operación máxima	Ejemplo
Categoría 1	Rango de Voz.	Cable de teléfono
Categoría 2	Datos a 4 Mbps	Token Ring a 4 Mbps
Categoría 3	Datos a 10 Mbps	Ethernet a 10 Mbps
Categoría 4	Datos a 20 Mbps	Token Ring 16 Mbps
Categoría 5	Datos a 100 Mbps	Fast Ethernet

Cuando se ha elegido el cable UTP, se requiere saber para que tipo de conexión se va a ocupar, para ello existen estándares que nos dicen como usarse y en que casos.

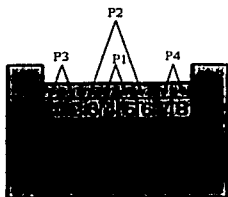
Existen dos estándares usados frecuentemente como referencia en el cableado estructurado; el EIA/TIA T568-A y el EIA/TIA T568-B de la ANSI. En ellos se definen la forma de organizar la disposición de los hilos de los cables y el uso de cada uno de ellos.

Los cables UTP contienen 4 pares de hilos identificados por colores. Un par se forma de un hilo de un color y el otro de ese mismo color con blanco. Cada cable tiene su función específica; algunos sirven para transmitir y otros para recibir información.

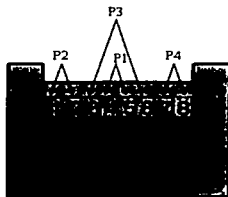
Nosotros utilizaremos cable UTP categoría 5, ya que usaremos Fast Ethernet.

A continuación se muestran los diagramas los conectores RJ45 vistos de frente con estas dos normas, luego la manera en que se utilizan y los usos para los que se destina.

TESIS CON  
FALLA DE ORIGEN



EIA/TIA T568-A



EIA/TIA T568-B

Figura 8.9.1.1. Diagramas del cableado T568-A y T568-B

EIA/TIA T568-A		
Pin	Par	Color
1	3	Blanco/Verde
2	3	Verde
3	2	Blanco/Naranja
4	1	Azul
5	1	Blanco/Azul
6	2	Naranja
7	4	Blanco/Café
8	4	Café

Tabla 8.9.1.1. Código de colores EIA/TIA 568-A

EIA/TIA T568-B		
Pin	Par	Color
1	2	Blanco/Naranja
2	2	Naranja
3	3	Blanco/Verde
4	1	Azul
5	1	Blanco/Azul
6	3	Verde
7	4	Blanco/Café
8	4	Café

Tabla 8.9.1.2. Código de colores EIA/TIA 568-B

Los tipos de patch cord comunes de uso en una red se derivan a partir de estos dos estándares. Para hacerlos es necesario utilizar herramienta especial como ponchadoras de la medida adecuada (RJ45), navaja y pinzas. Se pela el cable de manera que puedan entrar los hilos y se acomodan dentro del conector de acuerdo al estándar usado y luego se ponchan con la herramienta especial.

**Patch cord de conexión directa (Straight Through.)**

TESIS CON  
FALLA DE ORIGEN

Ambos extremos deben de estar armados de la misma manera cuando se observan los conductores. Es decir se deben tener la misma configuración de ambos lados, ya sea la T568-A o la T568-B. En Ethernet 10baseT o 100baseT solo se usan cuatro hilos.

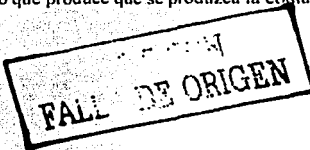
Este tipo de configuración se usa para:

- Conectar un enrutador a un Switch o Hub.
- Conectar un servidor a un Hub o Switch.
- Conectar una estación de trabajo a un Hub o Switch.

#### Patches de interconexión cruzada (Crossover.)

Un extremo del cable se debe armar según el estándar T568-A y el otro según el estándar T568-B. Esto hace que los pares de recepción y transmisión queden cruzados lo que produce que se produzca la comunicación. Este tipo de configuración se usa para:

- Uplinks ente Switches.
- Conectar Hubs con Switches.
- Conectar Hubs con Hubs.
- Conectar un puerto de enrutador a otro enrutador.
- Conectar dos terminales directamente.



#### Patch de consola (Rollover.)

Sirve para conectarse desde un puerto de consola de enrutador o Switch a una estación de trabajo que ejecute software de emulación de terminal.

La señalización y cableado del puerto de consola usan un Rollover y adaptador DB9, de acuerdo a la siguiente tabla:

Cable Rollover RJ45 a RJ45		Adaptador RJ45 a DB9
Desde el Pin:	Hasta el Pin:	Número de Pin DB9
1	8	8
2	7	6
3	6	2
4	5	5
5	4	5
6	3	3
7	2	4
8	1	7

Tabla 8.9.1.3. Configuración de cable Rollover.

Es probable que no tengamos que realizar este tipo de configuración ya que los equipos pueden venir con ellos.

#### Configuración del rematado en los paneles de parcheo.

Cuando el cableado va hacia un panel de parcheo la configuración en que se remata también sigue los estándares mencionados. Para rematar el cable se necesita de una herramienta adecuada llamada rematadora, la cual es un mango con navajas intercambiables apropiadas para cada tipo de cable.

Para hacerlo se colocan los hilos en la posición correspondiente dentro de los sujetadores dentro de cada puerto en el panel de parcheo y una vez ubicados se rematan para que queden fijos.



### 8.9.2 Cableado V.35

No describiremos como se elabora este tipo de cable, ya que su construcción es mucho más delicada. Por lo tanto este tipo de cable se tiene que adquirir ya hecho, aunque su precio es alto.

### 8.9.3 Cableado coaxial BNC.

El cableado coaxial BNC es más simple que el UTP, ya que solo se tienen dos conductores eléctricos.

Para rematar cualquier tipo de coaxial solo es necesario pelarlo adecuadamente y rematarlo con la pinza especial para cada medida de conector.

### 8.9.4 Etiquetado.

En lo que se refiere al etiquetado de cables se sugiere usar una etiquetadora para poder identificar fácilmente los extremos de cada cable, usando una nomenclatura única para evitar ambigüedades.

Se sugiere que sea de la siguiente manera e incluya:

- Tipo de cable. (Tecnología, si es cruzado o uno a uno)
- Número identificador de cable.

En el caso de "patch cords" o cables sueltos y cortos para los paneles de parcheo, no es necesario poner una etiqueta en cada extremo del cable, ya que uno solo es suficiente.

Una etiqueta de ejemplo es la siguiente:

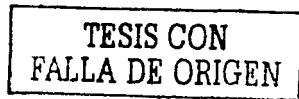


Figura 8.9.4.1 Etiqueta de ejemplo para cables UTP.

Dicha etiqueta se adhiere en cada extremo del cable o en uno solo según sea el caso.

En lo que se refiere al etiquetado de puertos en los paneles de parcheo, la etiqueta se coloca debajo de cada puerto siguiendo el orden de numeración mencionado anteriormente de acuerdo al tipo de panel de parcheo.

Para facilitar la ubicación del puerto en la otra punta del cable se sugiere usar la siguiente numeración:

En el rack de parcheo se nombran los paneles según el orden correspondiente al tipo de panel con una letra mayúscula, empezando por la A en los paneles RJ45 y continuando la lista en los BNC y terminando en los V.35

Cada puerto en cada panel se numera según el orden mencionado de acuerdo al tipo de panel, empezando por cero y reiniciando la numeración en cada panel.

De esta manera se tiene que para el panel RJ45 superior, los puertos van desde el A-0 al A-15 en el caso de que se tengan 16 puertos en ese panel. Y así sucesivamente con cada panel.

Para continuar con el cableado y la numeración de los otros racks es necesario que cada panel contenga solamente conexiones provenientes de un solo rack, es decir que aunque sobren puertos después de haber cableado un rack en particular con el de parcheo no se ocupen para cablear otro rack sino que se utilice otro panel.

En los paneles de los racks restantes, ya que solo llegan sus cables a un solo panel se colocaran las etiquetas con la misma nomenclatura que en el rack de parcheo, es decir si en el rack 3 en el cableado UTP los cables ocupan los puertos C-0 al C-13, entonces el panel tenga los mismos números.

De esta manera el rack de parcheo sirve de referencia para todos los otros racks y se pueden localizar fácilmente ambos extremos.

De ser posible también se pueden colocar etiquetas en los cables para añadir más información.

Los paneles de parcheo en los racks generalmente vienen con lo necesario para poner etiquetas que identifiquen los cables que se conectan a ellos.

### 8.10 Ejemplo de implementación.

El ejemplo de implementación que proponemos se basa en la distribución propuesta en el capítulo anterior, a partir del cuál se calcula el cableado necesario para hacer funcional dicha configuración. Entre ello se proponen los cables siguientes.

El número de cables y puertos propuestos, es el mínimo redondeado de acuerdo a las características de los equipos instalados en cada rack, a un número superior de puertos de acuerdo a las características de los patch paneles usados.

Como todo el cableado de datos fijo se dirige al rack de paneles de parcheo, se muestra la correspondencia de cables de cada uno de los racks al rack antes mencionado.

Del Rack0 a:	Tipo de cable.		
	Cable UTP.	Coaxial.	V.35
Rack1	32	8	48
Rack2	32	8	48
Rack3	32	8	48
Rack4	16	8	32
Rack5	16	8	32
Rack6	64	8	64

Suponiendo que cada dispositivo tiene la capacidad máxima de puertos mostrada.

Dispositivo	Puertos		
	RJ45	BNC	V.35
AGS+ <sup>(1)</sup>	16	0	16
500-CS	16	0	0
WS-C1201	8	0	0
3000 <sup>(2)</sup>	1	0	0
4000	1	0	6
7000 <sup>(3)</sup>	1	0	16

<sup>(1)</sup> En este dispositivo de puede tener la combinación de 4 diferentes tarjetas, cada tarjeta puede tener 4 o 8 puertos V.35, 8 puertos Ethernet, 4 puertos Token Ring, 2 FDDI, etc. En este caso se consideran que son 2 tarjetas con 8 puertos V.35 y 2 tarjetas con 8 puertos Ethernet.

<sup>(2)</sup> 2 puertos Ethernet (AUI) y puerto de consola RJ45.

<sup>(3)</sup> En este dispositivo de puede tener la combinación de 5 diferentes tarjetas, cada tarjeta puede tener 8 puertos V.35, 8 puertos Ethernet, 4 puertos Token Ring, 2 FDDI, etc. En este ejemplo se consideran 2 tarjetas con 8 puertos V.35.

Cada tipo de cable debe de ser rematado en los puertos del tipo correspondiente, según el orden y numeración sugeridos.

### 8.11 Resumen.

Se puede resumir brevemente que el cableado que se instalará para hacer funcional y práctico el laboratorio debe ser planeado y documentado apropiadamente, permitiendo así un uso eficiente de los equipos que se encuentran instalados en el laboratorio.

---

Se necesitarán usar diferentes tipos de cableado y de interfaces, por lo que es importante saber cuáles son necesarias para poder interconectar correctamente los equipos instalados, de acuerdo a las características de cada uno.

El número de puertos necesarios para cada tipo de interfaz, se tendrá una vez que se tenga la distribución definitiva de los equipos en cada rack y el número de tarjetas que tengan los equipos.

---

## Capítulo 9

### 9 Equipamiento del laboratorio.

#### 9.1 Introducción.

El equipamiento con el que contará el laboratorio se refiere a los equipos necesarios para llevar a cabo las labores de operación para las que fue diseñado, así como labores de mantenimiento y solución de fallas. Entre éstos equipos están los dispositivos de red, tales como equipos de comunicaciones y equipos terminales, además de equipamiento con fines didácticos que complementa las labores del laboratorio. Los dispositivos de red se pueden clasificar de acuerdo a su función dentro de la red de datos, dicha clasificación tiene por un lado a los equipos de comunicaciones de datos y por el otro a los equipos terminales de datos.

Los equipos de comunicaciones que tienen como función principal el transportar la información en forma de datos digitales a través de la red hasta los equipos terminales. Tales equipos se les conoce también como DCE's por sus siglas en inglés (Data Communication Equipment.)

En éste capítulo se dará una visión general de qué son y qué hacen los equipos con los que trabajaremos y que caen dentro de ésta categoría, lo cual junto a las bases teóricas expuestas en la primera parte y algunos elementos más que se plantearán en los siguientes capítulos nos permitirán hacer el diseño lógico y físico de la red del laboratorio de datos.

Los equipos terminales son aquellos donde se encuentra la aplicación o servicio final al cuál se requiere acceder y pueden encontrarse distribuidos de diversas maneras. Tales equipos se les conoce también como DTE's por sus siglas en inglés (Data Terminal Equipment.)

#### 9.2 Equipos de comunicaciones (DCE's.)

Los equipos de comunicaciones de datos (DCE's) son aquellos dispositivos de red, que se encargan de tareas como el establecer, mantener y finalizar conexiones de transmisión de datos, así como otras tareas opcionales tales como procesamiento, cifrado, filtrado, monitoreo de los datos, etc. con el fin de que los datos sean transmitidos correcta y eficientemente de un equipo terminal a otro y de ser necesario, dar servicios adicionales a los mismos.

Por estar destinados a proveer comunicaciones entre los equipos terminales, son equipos intermedios, pero no menos importantes, ya que sin ellos no sería posible transmitir información de un lugar a otro.

Los equipos de comunicaciones deben de satisfacer las necesidades requeridas por los servicios y aplicaciones existentes en los equipos terminales, las cuales pueden ser poco o muy demandantes de recursos de la red, por ejemplo una aplicación de correo electrónico no necesita un gran ancho de banda para transmitir los mensajes, así como tampoco le importará si hay un retraso evidente en la transmisión de datos, ya que éstos no son de alta prioridad; sin embargo una aplicación de telefonía sobre IP no permitiría un gran retraso o "delay" en la transmisión de los paquetes de datos, y más allá todavía, una aplicación de videoconferencia además de no permitir retraso en los datos, requiere de un ancho de banda muy grande y una calidad de servicio (QoS) bien definida.

En la red, pueden existir gran diversidad de aplicaciones, de las cuáles, cada una tiene sus propios requerimientos en cuanto al desempeño que requieren que la red tenga, y además dicha red deberá cumplir con todas estas expectativas con las aplicaciones posiblemente ejecutándose simultáneamente.

Aunque en nuestro caso, para el diseño de la red no podemos partir de un análisis de las necesidades que debemos satisfacer en cuanto a las aplicaciones que deben de existir, es necesario conocer términos que más adelante nos servirán como base para poder configurar y optimizar correctamente nuestro diseño de red.

Estos aspectos se conocen como metas técnicas y limitaciones de la red, y es necesario conocerlas para poder hacer una buena selección y uso de los equipos de red, que aunque ya estén elegidos, se requieren también para poder saber qué podemos obtener de ellos.

Entre estas metas técnicas, están la escalabilidad, la disponibilidad, el desempeño, la seguridad, la manejabilidad, la adaptabilidad y el costo-eficiencia, las cuáles serán abordadas más adelante.

---

Los equipos DCE's que se tienen contemplados para el laboratorio son enrutadores Cisco de diversos modelos y por tanto de diversas características y capacidades, además de switches, Hubs y posiblemente Bridges y fraccionadores.

Aunque no podemos elegir los equipos con los que vamos a implementar el laboratorio, por estar estos ya definidos, aun así es importante saber qué características son las más importantes para reconocer las capacidades de cada uno de ellos, y una vez que se conozcan las características de cada uno, saber de qué manera se puede optimizar su uso y explotar todas las funciones que son capaces de desempeñar.

Para elegir dispositivos de red en general se contemplan los siguientes criterios:

- **Número de puertos.**

Es el número de interfaces de determinado tipo con las que cuenta el equipo, es necesario saber con cuántas cuenta, ya que a través de cada una de ellas se podrá hacer una conexión con otro equipo.

- **Velocidad de procesamiento.**

Depende directamente del tipo de procesador y circuitería interna con la que cuente el equipo, y determina la cantidad de operaciones que puede realizar en determinado periodo de tiempo. Dicho procesamiento puede ser desde la actualización de tablas de enrutamiento, manejo de sesiones, cálculo de rutas, filtrado, etc. Dependiendo del tipo de tarea que desempeñe dicho equipo en la red.

- **Latencia ("Latency") o retardo de tránsito.**

Es el retraso entre el tiempo en que un dispositivo requiere acceso a la red y el tiempo en que se le da permiso para transmitir y depende del tipo de acceso al medio, de la tecnología de red, de la prioridad de transmisión del dispositivo si es soportada dicha característica, etc.

- **Tecnologías LAN soportadas (Ethernet, Token Ring, FDDI, etc.)**

La variedad de tecnologías varía de acuerdo a las necesidades y soluciones que se quieran implantar. El tener varias tecnologías diferentes implica diversidad en los equipos necesarios para poder trabajar con ellas en conjunto.

- **Autosensado de la velocidad.**

Es la capacidad que un equipo tiene para determinar la velocidad de transmisión en el medio y poder operar automáticamente en ella, sin necesidad de configuraciones adicionales. Esto es debido a que hay tecnologías que son capaces de hacerlo en varias velocidades, tal como Ethernet (10, 100, 1000 Mbps) o Token Ring (4 o 16 Mbps.)

- **Medios de cableado soportados.**

Son la variedad de interfaces y cables soportados, y pueden ser desde cable UTP, coaxial, serial, fibra óptica, etc, y dependen de la tecnología de red usada.

- **Facilidad de configuración.**

Es un factor que determina qué tan complejo puede llegar a ser el poner en marcha, configurar y optimizar el funcionamiento del equipo. Depende fundamentalmente de cómo haya enfocado esto cada fabricante y que tantas herramientas ponga en manos del usuario para hacerlo.

- **Manejabilidad.**

Es la facilidad con la que la red puede ser manejada y monitoreada, incluyendo la administración del desempeño de la red, de las fallas, configuración, seguridad y capacidad de auditoría. Y es manejada a través de diversos protocolos diseñados para tal tarea, como SNMP o RMON.

- **Costo.**

---

Aunque en nuestro caso ya no es importante este aspecto directamente, dado que los equipos para el laboratorio ya están destinados, es un factor que siempre se toma en cuenta para la adquisición del equipo, y puede ser analizado desde varias perspectivas como costo por puerto, costo anual, etc.

- Soporte para fuentes de poder redundantes.  
En redes donde la disponibilidad de los servicios es indispensable, debido al tipo de información manejada, es importante tener redundancia también en las fuentes de poder que alimentan al sistema.

En nuestro caso no es tan relevante el objetivo de tener una alta disponibilidad de la red, pero es necesario saber si el equipo cuenta con esta característica.

- Disponibilidad y calidad de soporte técnico.  
Cuando se adquieren equipos es necesario saber si éstos tienen incluido soporte técnico en caso de problemas en la puesta en marcha y configuración de los equipos. Los equipos que se van a ocupar en el laboratorio ya no tendrán este tipo de soporte vigente, por lo que se tendrá que hacer uso de la documentación impresa y la disponible en medios electrónicos.

- Disponibilidad y calidad de la documentación.  
Los equipos deben de contar con la documentación técnica necesaria para poder instalar, configurar y resolver problemas en los equipos, y ésta puede ser accedida en forma impresa o en forma electrónica como página Web en la página del fabricante.

- Disponibilidad y calidad de entrenamiento (para enrutadores y switches complejos).  
Algunas empresas ofrecen entrenamiento especializado en los equipos adquiridos, a los que se encargarán de operar el equipo que generalmente son los administradores u operadores de la red, esto es un servicio añadido que se debe considerar si se quiere adquirir un equipo de estos, sin embargo a nosotros ya no nos compete esto ya que los equipos con los que se va a trabajar no son nuevos.

- Reputación y fiabilidad del vendedor.  
De la reputación y fiabilidad del vendedor depende la confianza que se pueda tener en la garantía, el soporte, la documentación y la calidad del equipo adquirido, por lo que es necesario saber las referencias del vendedor que suministra o fabrica tales equipos.

- Disponibilidad de resultados de pruebas que confirmen el desempeño del dispositivo.  
Las empresas fabricantes de estos equipos, generalmente ponen a libre disposición las pruebas y los resultados de ellas, aplicadas a sus equipos además de hacer comparativas con otros equipos similares de otros fabricantes, en las cuáles se muestran las características operativas de los equipos.

A continuación se hará una breve descripción de cuáles son las funciones principales de cada uno de los dispositivos que cae en la categoría de DCE's y su tarea a desempeñar en la red.

### 9.2.1 Enrutador.

Un enrutador como ya se dijo, es un equipo de comunicación de datos, el cuál tiene varias funciones en la red, entre ellas la principal es la de enrutar los paquetes de datos generados en una red local a través de líneas digitales a otros equipos hasta llegar a su destino en otra red. De esta manera se puede ver que un enrutador sirve para conectar redes LAN.

Un uso que se le puede dar, es el de segmentar y dividir redes a través de cada una de sus interfaces, esto con el fin de reducir el dominio de colisiones y el dominio de broadcast, con lo cual se mejora el desempeño de la red local.

Cada enrutador es responsable de crear y mantener actualizadas tablas de enrutamiento para cada protocolo de red. Dichas tablas son creadas a partir de protocolos de enrutamiento, y pueden ser estáticas o dinámicas. De esta manera el enrutador extrae de la capa de red la dirección destino del paquete y realiza una decisión de envío basado en el contenido de la tabla de enrutamiento para ese protocolo.

---

La inteligencia del enrutador y de los protocolos de enrutamiento, permiten seleccionar la mejor ruta, basándose en diversos factores como pueden ser; la cantidad de saltos necesarios para llegar a su destino, la velocidad de la línea sobre la cual ha de enviarse la información, el retraso, la carga de la red, etc, además de que puede proporcionar redundancia en las rutas para poder llegar de un punto de la red a otro.

Un enrutador actúa también en el aspecto de la seguridad de los datos, esto es que permite que solo máquinas autorizadas transmitan datos hacia y desde fuera a la red, manteniendo la seguridad y privacidad de la información. Los enrutadores también manejan errores, mantienen estadísticas de uso de la red, y manejan algunos aspectos de la seguridad.

Un enrutador puede funcionar como puente o Bridge, para realizar este tipo de tarea, debe contar con el software y el hardware adecuado, así como una configuración apropiada para realizar tanto enrutamiento como puenteo o "bridging".

Las nuevas generaciones de switches también pueden realizar funciones de la capa de red por lo que se les llama switches de capa 3, sin embargo dadas sus funciones deben de ser considerados como enrutadores, aunque debe hacerse notar que los switches realizan la tarea de conmutación a nivel de hardware y los enrutadores a nivel de software.

Para elegir un enrutador los siguientes criterios pueden ser añadidos a los ya mencionados para un dispositivo de red:

- Protocolos de capa de red soportados.

Son los protocolos de red que el enrutador puede soportar, y son tratados con más profundidad en el capítulo dedicado a las tecnologías y protocolos a soportar en el laboratorio.

- Protocolos de enrutamiento soportados.

Estos se encargan de determinar las mejores rutas para poder enviar la información con los protocolos enrutables, e igualmente serán tratados con más detalle en el capítulo dedicado a las tecnologías y protocolos a soportar en el laboratorio.

- Soporte para aplicaciones multimedia (RSVP, IP multicast, servicios garantizados)

Este tipo de soporte permite, que los recursos o limitaciones de la red sean administrados o controlados de mejor manera a fin de permitir la operación de aplicaciones con necesidades bien definidas de ancho de banda, distorsión entre líneas, retraso, etc., es decir que permitan ofrecer calidad de servicio.

- Soporte para encolamiento avanzado, switcheo y otras tareas de optimización.

Estas son tareas avanzadas que buscan mejorar la transmisión de los datos en la red.

- Soporte para compresión.

Es la capacidad que tiene el enrutador para que a través de un algoritmo, reducir el espacio requerido para almacenar la información así como reducir el ancho de banda necesario para transmitir los datos.

- Soporte para cifrado.

El cifrado es un proceso que codifica datos para protegerlos de ser leídos por cualquiera que no sea el receptor destinado. Este proceso requiere de un dispositivo capaz de cifrar y otro de descifrar a través de una llave.

El principal beneficio es el de dar mayor seguridad a los datos aunque requiere mucho procesamiento.

- Soporte para filtrado de paquetes y otras características avanzadas de Firewall.

Ésta es una característica enfocada a la seguridad de la red y de lo que de ella depende, y será vista con más detalle en el futuro cuando se trate el tema de seguridad.

**Componentes del enrutador.**

Físicamente, un enrutador consta de diversos componentes, entre los más importantes están los siguientes:

---

- El chasis, que es la estructura que contiene y protege todos los demás componentes y además se puede montar a muebles como racks o gabinetes para dar más estabilidad al sistema.

- Procesador o CPU. Éste se encuentra en las tarjetas procesadoras que se encargan de tareas como ejecutar el sistema operativo, administrar los recursos y controlar procesos como el de hacer cálculos de rutas, filtrado de paquetes, actualización de tablas de enrutamiento, etc.

El enrutador como cualquier otra computadora necesita una CPU, la cual varía en cada serie y modelo de enrutador.

- Las interfaces. Todo enrutador tiene interfaces, algunas de los tipos de interfaces en enrutadores Cisco son Ethernet, Fast Ethernet, Token Ring, FDDI, Seriales de alta y baja velocidad, HSSI e ISDN, entre otras.

- Puerto de consola.

Todos los enrutadores tienen un puerto de consola. Dicho puerto proporciona una conexión serial asincrónica (EIA/TIA-232 o también conocida como RS232), que nos permite comunicarnos con el enrutador y configurarlo.

El tipo de conexión física al puerto de consola depende del modelo de enrutador. Algunos usan un conector hembra DB25 y otros un conector RJ45. Como regla general los enrutadores de modelos menores tienen un conector de consola RJ45.

- Puerto auxiliar.

La mayoría de los enrutadores tiene un puerto auxiliar, que al igual que el puerto de consola nos permite comunicarnos con el enrutador.

El puerto auxiliar es frecuentemente usado para la conexión de un modem para administración del enrutador "out-of-band" o fuera de banda. Un camino "out-of-band" no lleva paquetes enrutados, es usado principalmente para acceder un enrutador cuando una ruta de red o circuito falla.

- La memoria también es un componente indispensable, dentro de un enrutador hay varios tipos de memoria, entre las cuáles hay 4 tipos, que son ROM, Flash, RAM y NVRAM.

La memoria ROM es donde normalmente se almacena el software de arranque del enrutador. El cual se encarga de iniciar el equipo, generalmente es uno o más chips en la tarjeta procesadora del equipo.

La memoria Flash tiene como propósito almacenar el software del IOS que el enrutador va a ejecutar. Puede ser una SIMM o una tarjeta PCMCIA.

La memoria RAM es usada para hacer muchas cosas, entre las principales están las tablas de sistema y buffers del IOS. Es la única que pierde su contenido cuando es el enrutador es reiniciado

La NVRAM o RAM no volátil sirve para almacenar la configuración que el IOS lee para arrancar el sistema.

- La fuente de poder, que es la encargada de regular y convertir la energía que se suministra al equipo a través del suministro eléctrico y la distribuye a cada uno de los componentes que lo necesite. Algunos equipos, dependiendo de su tamaño pueden tener fuentes dobles a fin de tener redundancia en caso de falla

En el aspecto del software o sistema operativo, éste determina qué funciones puede realizar el enrutador, así como los protocolos soportados por él. Esto es, que cada enrutador cuenta con un sistema operativo de red (IOS), que es el encargado de administrar y controlar todas las tareas que realiza el mismo.

Los protocolos y funciones más específicas que puede manejar un enrutador a través del sistema operativo, serán analizados más a detalle en otros capítulos. Incluyendo configuración del sistema, protocolos enrutables, protocolos de enrutamiento, direccionamiento, etc.

### 9.2.2 Bridges.

Un puente o Bridge es un dispositivo que conecta y pasa tramas entre dos segmentos de red. Este dispositivo opera en la capa 2 del modelo de referencia OSI y filtra, envía o rechaza una trama entrante basado en la dirección MAC de destino de la misma, a diferencia de un enrutador, el puente no mira la información encapsulada de capa 3 o superior que viene en la trama recibida.

El puente segmenta dominios de ancho de banda, de manera que los dispositivos en lados opuestos del puente no compiten entre ellos por el control de acceso al medio, sin embargo no segmenta los dominios de



---

broadcast, a menos que sea programado para filtrarlos. Para evitar tráfico excesivo de broadcast, se deben segmentar las redes de switches y bridges con enrutadores o dividirlos en VLAN's.

Un puente es un dispositivo "store and forward", es decir que cuando el puente recibe una trama, espera a recibirla completa, para poder determinar a través de cual puerto ha de ser reenviada

Para elegir un bridge, los siguientes criterios pueden ser añadidos a los ya mencionados para un dispositivo de red:

- Tecnologías de bridging soportadas ("transparent bridging", "spanning tree-algorithm", "source routing bridging", etc.)

El esquema de "transparent bridging" es usado frecuentemente en redes Ethernet e IEEE 802.3 en la cual los bridges pasan las tramas a lo largo de un salto a la vez, basado en tablas que asocian nodos finales con puertos del bridge. El puenteo transparente ("transparent bridging") es así que nombrado porque la presencia de puentes es transparente a los nodos del final de la red.

En redes relativamente grandes, podemos encontrar una topología o estructura sumamente compleja, donde la coexistencia de varios puentes y múltiples segmentos puede dar lugar a la formación de bucles en la emisión de tramas.

El "Spanning Tree algorithm" es un algoritmo bajo la normativa IEEE 802.1 d, que es una técnica que establece un protocolo de comunicación entre los puentes para evitar las conexiones redundantes y almacenar tan sólo aquellas conexiones más importantes, de acuerdo a criterios de rapidez y economía, con lo que se consigue tener redes sin bucles.

El "source routing bridging" es un método de puenteo originado por IBM que es popular en redes Token Ring. En el cuál una estación final fuente determina la ruta al destino requerido al enviar una trama exploradora.

La información sobre estas tecnologías puede ser ampliada en la página de Cisco.

- Tecnologías WAN soportadas.

Son las tecnologías usadas como opciones típicas para conectar sitios geográficamente dispersos, entre tales tecnologías están SONET (Synchronous Optical Network), ATM, Frame Relay, SMDS (Switched Multimegabit Data Service,) etc.

- El número de direcciones MAC que el puente puede aprender.

Entre más grande sea este número, es mayor la capacidad que tiene el equipo para trabajar en redes más grandes o con más equipos interconectados.

- Soporte para filtrado.

Esta capacidad permite seleccionar las tramas que pueden pasar o no, brindando más funcionalidad y seguridad a la red.

Los protocolos y funciones más específicas que puede manejar un bridge serán analizados más a detalle en otros capítulos. Incluyendo configuración del sistema, la diferentes técnicas de puenteo, la integración con otros dispositivos de red, etc.

### 9.2.3 Switch.

Un Switch es un dispositivo de red que filtra, envía y realiza el reenvío de tramas según la dirección destino en cada una. La manera en que lo hace es a través de la dirección MAC de destino que se encuentra en la trama recibida.

---

Las funciones que realiza un Switch, están comprendidas hasta la capa 2 del modelo de referencia OSI. Aunque el término de switches de capa 3 está muy difundido, éstos no son realmente switches, sino enrutadores, por tanto se consideran como tales.

El Switch puede resolver problemas de rendimiento en la red, que son debidos a anchos de banda pequeños y embotellamientos, ya que el Switch puede agregar ancho de banda, acelerar la salida de paquetes y reducir el tiempo de espera o "latencia".

El Switch segmenta la red al reducirla a pequeños dominios de colisiones, por lo que reduce o casi elimina la competencia de los dispositivos por el acceso al medio, al dar a cada uno que este conectado a cada puerto, un ancho de banda dedicado.

Los switches tienen la capacidad de hacer procesamiento "cut and through" o "store and forward". Con el procesamiento "cut and through" se mira rápidamente la dirección destino en el primer campo de la trama entrante, luego se determina el puerto de salida e inmediatamente se empieza a enviar bits al puerto de salida. Sin embargo si el medio de transmisión no es fiable y los datos frecuentemente tienen errores, éste método no debe ser usado.

Algunos switches tienen la capacidad de moverse automáticamente de "cut and through" a "store and forward" cuando un umbral de errores permitidos es sobrepasado, y luego regresan cuando se vuelve al umbral permitido. Ésta característica es llamada "cut and through" adaptivo.

Cuando se trata de elegir un Switch, los siguientes criterios pueden ser añadidos a los mencionados para un dispositivo de red:

- Throughput soportado en paquetes por segundo.

Es la cantidad de datos reales que se transmiten en un determinado tiempo, es decir la información transmitida sin contar con los encabezados y colas que añade cada capa.

- Soporte para switcheo "cut and through".

Es la capacidad del Switch para poder enviar una trama tan pronto como la vaya recibiendo, es decir que puede enviar la trama sin necesidad de haber terminado de recibirla, a diferencia de cuando se hace en la forma "store and forward", en la que la trama se envía una vez que ha sido recibida completamente, para hacer esto es necesaria más inteligencia por parte del Switch.

- Soporte para switcheo "cut and through" adaptivo.

El switch "cut and through" adaptivo es aquel en que el Switch conmuta entre el método "cut and through" y el "store and forward", dependiendo de la cantidad de errores en las tramas enviadas, ya que si la cantidad de errores es mayor que cierto umbral, el Switch decide enviar las tramas por "store and forward" hasta que la cantidad de errores baje del umbral permitido, y entonces vuelve a enviar las tramas por "cut and through".

- Auto detección de operación en half o full duplex.

Es la capacidad que tiene de detectar si el modo de transmisión en un instante preciso es unidireccional o bidireccional, y cambiar de un modo a otro.

- Tecnologías VLAN soportadas.

Son las tecnologías con las cuáles se pueden crear LAN virtuales, es decir hacer que grupos de dispositivos en segmentos diferentes de la red se comporten como si estuvieran en el mismo, usando una misma infraestructura física común.

- La memoria disponible para tablas de switcheo, para tablas de enrutamiento (en el caso de que el Switch tenga un modulo de enrutamiento.) Y la memoria para rutinas de los protocolos soportados.

La memoria depende directamente del hardware que tenga el Switch, y entre más memoria tenga, tiene más facilidad para poder ejecutar tareas que demanden de éste recurso.

- Disponibilidad de módulos de enrutamiento.

El que los switches tengan módulos de enrutamiento los convierte en enrutadores, con lo que adquieren más inteligencia para reenviar las tramas, ya que pueden evaluar mejor las rutas para enviar las tramas que solo la tabla de direcciones MAC.

Los diferentes protocolos y técnicas de switcheo serán tratados en otro capítulo, así como éstas se integran con los demás protocolos que va a existir en la red.

#### 9.2.4 HUBs o concentradores.

Un HUB o concentrador es un dispositivo que sirve como punto de conexión común para dispositivos dentro de una red, normalmente unen a segmentos de una red. El HUB se encarga de distribuir la información recibida por cualquiera de sus puertos a todos los demás, por lo que define un dominio de broadcast, es decir que lo que entre por cualquiera de sus puertos, es retransmitido por todos los demás.

Existen varios tipos de HUB:

- Pasivo, simplemente actúa a modo de repetidor de datos entre todos sus puertos.
- Gestionable, permite monitorizar su actividad y configurar puertos y tráfico en su red.

El HUB trabaja fundamentalmente en la capa 1 del modelo de referencia OSI. Y es el elemento más simple con el que se podría construir una red simple, que solo podría ser plana, lo cual ocasiona problemas de tráfico y saturación de los recursos de la red.

La topología con la que trabaja el HUB es de estrella, ya que todos los dispositivos se conectan a él de la misma forma y sin jerarquía alguna.

#### 9.2.5 Fraccionadores.

Un fraccionador es un equipo de comunicaciones que funciona como un multiplexor para transmitir enlaces digitales de un punto a otro.

Es capaz de manejar enlaces digitales de diversas velocidades y segmentarlos en canales y anchos de banda seleccionables.

Entre los tipos de enlaces que puede manejar están E1's, T1's y sus fracciones, con lo que es posible dividirlos en canales con anchos de banda múltiplos de 56 y 64 kbps.

Otra de sus funciones es cambiar de un tipo de interfaz a otra, como por ejemplo coaxial a V.35, dependiendo de las características e interfaces de cada equipo en particular.

#### 9.2.6 Metas técnicas y limitaciones de los dispositivos de red.

Las metas técnicas y limitaciones de los dispositivos de red deben ser conocidas a fin de poder saber, qué es lo que podemos hacer y obtener con ellos en una red de datos. Esto se debe a que para poder hacer el diseño de una red y por tanto uso de los dispositivos mencionados se debe saber para qué se quiere y qué se planea obtener o qué problemas resolver con ella.

A continuación se nombran y se explica éstos conceptos y la terminología empleada para entenderlos.

##### 9.2.6.1 Escalabilidad.

Se refiere a qué tanto crecimiento puede tener un diseño de red y que tan fácil puede adaptarla a los cambios futuros. Este es un aspecto importante para empresas o instituciones grandes con muchas posibilidades de crecimiento. Es decir que continuamente se están añadiendo usuarios, aplicaciones, sitios adicionales y conexiones externas a una alta velocidad.

Si se tiene estas condiciones, los equipos que se deben de usar deben de poder ser altamente escalables.

Las dificultades vienen cuando se seleccionan las tecnologías para lograr la escalabilidad, ya que puede ser un proceso complejo de planeación.

##### 9.2.6.2 Disponibilidad.

La disponibilidad se refiere a la cantidad de tiempo que la red o los equipos están operacionales y disponibles para los usuarios, lo cuál puede ser un objetivo primordial dependiendo de las necesidades que se tengan. Ésta puede expresarse como un porcentaje de disponibilidad por hora, por día, por mes, o por año.

Un factor importante en la disponibilidad es el qué tan rápido se puede recuperar un equipo de una caída en el servicio.

La disponibilidad de la red también depende de la redundancia de equipos que exista, aunque si nos enfocamos a disponibilidad de un equipo en particular esto tiene otro enfoque. En adición a expresar la disponibilidad como un porcentaje de tiempo en estado operacional, se puede definir la disponibilidad como el tiempo Medio Entre Fallas o MTBF por sus siglas en inglés (Mean Time Between Failure), y el tiempo medio para reparar o MTTR por sus siglas en inglés (Mean Time To Repair.)

MTBF es un término que viene de la industria de las computadoras y es mejor expresado como cuánto tiempo estará operacional el dispositivo antes de caerse.

Cuando se habla de disponibilidad en el campo de redes, el MTBF es a veces designado como tiempo medio entre corte de servicio MTBSO (Mean Time Between System Outage.)

Aunque en nuestro diseño no es tan importante la disponibilidad como lo sería en una red corporativa, es una buena idea identificar las metas de disponibilidad que se pueden alcanzar para aplicaciones o servicios específicos. Pero además debe visualizarse que una alta disponibilidad significa un alto costo para lograrlo.

Muchos fabricantes de enrutadores, switches y Hubs, así como publicaciones comerciales especializadas, proveen en las especificaciones del producto figuras del MTBF y el MTRR.

### 9.2.6.3 Desempeño de red.

El desempeño de la red es tratado en muchas partes con un enfoque matemático, sin embargo solo lo describiremos brevemente, evitando el uso de ecuaciones y dándole un enfoque más práctico.

Hay muchas variables que intervienen en la valoración del desempeño de la red, la siguiente lista nombra las más importantes y describe brevemente cada una.

- Capacidad. (Ancho de Banda)

Es la capacidad de transporte de datos de un circuito o red y es usualmente medida en bits por segundo (bps.)

El ancho de banda es una de las características más planeadas de una red, aunque en nuestro caso no tiene tanta prioridad.

Puede decirse que en este aspecto, solo es necesario tener el ancho de banda necesario para lo que se necesita, ya que si se tiene en exceso, incrementa directamente el costo de los equipos y de una red.

- Utilización.

La utilización se puede clasificar según el tipo de recurso usado, los más importantes son los siguientes:

Uso de CPU	Es una medida instantánea del porcentaje del uso del procesador. Un procesador nunca debe de trabajar al 100% de su capacidad por periodos largos, ya que indica que esta sobrecargado lo cuál ocasiona fallas en los procesos que están ejecutándose.
Uso de Memoria.	Es el porcentaje de la memoria total del equipo en un instante dado o periodo de tiempo que se está usando para mantener los procesos en ejecución en el equipo así como los datos asociados dichos procesos.
Uso del ancho de banda.	Es una medida de cuánto ancho de banda es usado durante un periodo específico de tiempo y es comúnmente especificado como un porcentaje del ancho de banda. Hay herramientas de análisis de redes para medir y promediar el uso sobre un tiempo dado. El conocer la utilización de la red es un buen parámetro para evaluar la carga tanto en los equipos como un porcentaje de uso del procesador, como en la red, la cual puede ser causa de problemas, ya que si la carga excede un porcentaje recomendado surgen problemas de retraso, picos de tráfico, etc.

- **Throughput.**

El throughput está definido como la cantidad de datos libres de error y sin encabezados, que es transmitida por unidad de tiempo. Frecuentemente es definido para una sesión o conexión específica, pero en algunos casos el throughput total de una red es especificado. Idealmente el throughput debería ser lo mismo que la capacidad, pero no es el caso en redes reales.

Sin embargo, esta no es una medida que realmente muestre que tan buena es la red, por eso se usa también el término de throughput enfocado a la capa de aplicación. Es decir los datos de nivel de aplicación transmitidos netos sin contar la tasa de error, los encapsulados de los protocolos de cada capa, lo paquetes perdidos, etc.

- **Exactitud.**

La exactitud se refiere a que los datos recibidos en el destino sean los mismos que los enviados por la fuente. Para enlaces WAN o enlaces seriales la exactitud se mide como una tasa de error de bits o BER (BIT Error Rate.)

Para redes LAN, no se utiliza usualmente la BER, principalmente porque la transmisión entre hosts no está orientada a bit sino a tramas, por lo que si hay un bit erróneo en la trama entonces toda esta es errónea y debe de retransmitirse. El mecanismo para darse cuenta de ello es que el host transmisor calcula el CRC de los bits de datos encapsulados, y lo coloca en la en el campo CRC de la trama, luego el receptor calcula el CRC de los bits de datos recibidos, y comprueba que coincida con el CRC que viene en ella. Si no coincide, los datos contienen errores.

- **Eficiencia.**

La eficiencia es un concepto no muy claro en el campo de las redes, ésta compara cuántos bits se necesitan para transmitir en la red, para recibir una cantidad de bits de información útil o de capa de aplicación.

La eficiencia es afectada por todos los bits agregados para la encapsulación en cada capa, dependiendo de cada protocolo usado, es además afectado por la BER.

- **Retraso o "Delay".**

La cantidad de retraso en los datos transmitidos es una variable que evidentemente afecta aplicaciones multimedia como tales videoconferencia y telefonía sobre IP, las cuales requieren una variación mínima del retraso que los paquetes padecen.

La variación en el retraso se le conoce como "Jitter".

- **Tiempo de respuesta.**

El tiempo de respuesta es una variable que refleja el desempeño de la red, ya que es visible por parte del que la usa, en él interviene tanto el "Jitter", el retraso, el throughput, etc.

Un usuario humano empieza a notar retraso en el tiempo de respuesta alrededor de los 100 ms, si el tiempo de respuesta es menor, el usuario no notará el retraso.

El desempeño de la red se valora como el comportamiento de todas estas variables ya mencionadas, aunque algunas contribuyen más que otras y algunas son más difíciles de controlar.

#### **9.2.6.4 Seguridad**

Éste es uno de los aspectos más importantes en el diseño de una red empresarial o institucional, especialmente cuándo se tienen conexiones de Internet o Extranets. Esto es para evitar que cualquier problema interrumpa la capacidad de desarrollar sus actividades cotidianas y que los recursos e información valiosa sean dañados.

Este tema se abordará con mucha más profundidad en otros capítulos.

#### **9.2.6.5 Manejabilidad.**

Es la facilidad de poder realizar diferentes funciones como la administración del desempeño, de las fallas, de la configuración, de la seguridad y de la auditoría, es decir labores administrativas. Algunas de estas funciones pueden tener más peso que otras, dependiendo de los objetivos del sistema.

#### 9.2.6.6 Usabilidad.

Esta meta está relacionada con la manejabilidad, pero no es lo mismo, sino que se refiere a la facilidad de uso con la que cada usuario de la red puede acceder a ella y sus servicios.

La primera busca hacer que las tareas del administrador sean más fáciles, y la segunda que las tareas del usuario sean más fáciles.

#### 9.2.6.7 Adaptabilidad

Es la capacidad de que la red se adapte a nuevas tecnologías y cambios, en esto interviene el qué tan rápido los dispositivos se adaptan a problemas y actualizaciones, a patrones de tráfico cambiante, etc.

#### 9.2.6.8 Costo – eficiencia (“Affordability”.)

El objetivo de esta meta es llevar la máxima cantidad de tráfico por un costo financiero dado. Los costos financieros incluyen costos de equipamiento y costos de operación recurrentes. Es decir hace la valoración de la relación costo contra otras variables.

Hay una relación directa entre varias de las variables mencionadas anteriormente, para hacer el diseño de la red es necesario hacer un balance de todas estas metas técnicas y ver cuáles son más importantes en relación de otras.

Por ejemplo, para tener altas expectativas de disponibilidad se necesitan componentes redundantes, lo que eleva el costo de la implementación y la complejidad de la misma. Es por tanto necesario hacer un balance de cuáles se prefieren y cuáles se deben sacrificar.

### 9.3 Equipos terminales (DTE's.)

Los equipos terminales también conocidos por el acrónimo de DTE's (Data Terminal Equipment) son aquellos que transmiten y reciben datos de aplicaciones o servicios dentro de una red.

Tales DTE's pueden ser desde una terminal tonta hasta un equipo PC, o cualquier otra arquitectura de computadora que cuente con el hardware y protocolos necesarios para acceder a los equipos.

Los servicios a los cuales se puede acceder a través de estos equipos pueden ir desde aplicaciones de correo electrónico, acceso a páginas Web, telefonía sobre IP, videoconferencia, impresión remota y un sinnúmero de aplicaciones más, cada una con diversos requerimientos de ancho de banda, de retardo, de seguridad de los datos, etc.

Para ello es necesario que la red a la cual estén conectados los DTE's esté diseñada de tal forma que se cumplan con todos estos requerimientos de las aplicaciones corriendo en los equipos terminales, así como de los necesarios para la correcta operación y monitoreo de la misma red.

Debido a los alcances que se planea tenga el laboratorio, las aplicaciones con las que se pudiera contar en el laboratorio serían reducidas, ya que el objetivo primordial del laboratorio es brindar un espacio para el desarrollo de habilidades en protocolos de redes de datos, y no el de implementar una red completamente funcional con gran variedad de servicios como la que habría en una empresa o corporativo, para la cual se necesitarían más equipos y recursos y no vendría totalmente al caso ya que no es lo que buscamos.

Es necesario tener en cuenta que estos aspectos de desempeño para el diseño del laboratorio y de las prácticas que se realicen en el mismo, son muy importantes y se deben tener en cuenta si se quiere realmente conocer y familiarizarse con los protocolos de redes de datos.

Las aplicaciones soportadas por la red serán definidas más adelante una vez que se realice el diseño lógico de la red.

Entre los equipos terminales con los que contará el laboratorio estarán las terminales de acceso, él o los servidores instalados, alguna impresora y finalmente equipos para poder verificar la transmisión de datos de un punto de la red a otro y probar el funcionamiento de la misma. Tales equipos pueden ser estaciones de trabajo o Laptops para poder realizar transferencias de archivos por FTP o recepción de páginas Web por http o hasta teléfonos IP, según lo que se pueda obtener para equipar el laboratorio.

---

#### 9.4 Terminales de acceso.

Por terminales de acceso se van a entender como aquellos DTE's a través de los cuales se tenga acceso local o remoto a los equipos de comunicaciones o DCE's

A través de ellos se puede acceder por vía local o remota a los equipos que se encuentran instalados en el laboratorio, tales como los enrutadores y servidores, y efectuar algún tipo de configuración, de resolución de problemas, de actualización o de monitoreo de los mismos.

Una terminal de acceso puede ser casi cualquier equipo de computo que tenga implementado el conjunto de protocolos compatibles con la red o equipo al que se está conectando, y desde el punto de vista hardware puede ser desde un equipo PC o compatible, un servidor, una estación de trabajo, etc, siempre y cuando tenga una NIC o interfaz apropiada para conectarse a la red.

Por el lado del software la terminal de acceso puede estar ejecutando distintos sistemas operativos que tengan los protocolos y herramientas apropiados para ingresar a la red e iniciar una sesión, tales como MS-DOS, los diferentes sistemas UNIX existentes y similares, la familia MS Windows, OS/2, etc.

En la mayoría de los casos, las terminales de acceso van a ser la principal herramienta con la que se cuente para trabajar con los equipos del laboratorio y por tanto van a ser la principal herramienta con la que se va a trabajar. Por eso es importante planear desde el principio cuántas terminales serán necesarias para satisfacer la demanda de uso del laboratorio.

Se debe contemplar en la etapa de planeación del laboratorio el cómo se van a conectar dichas terminales para poder tener acceso a los equipos, sin embargo se dedicará un capítulo a definir de qué manera se hará esto.

Las características técnicas de los equipos que se usen como terminales de acceso se harán de acuerdo a los recursos con los que se contará una vez que se llegue a la etapa de implementación del laboratorio.

#### 9.5 Servidor Web.

El servidor Web es un equipo del tipo DTE, que por sus características y los servicios que deba ofrecer una vez que el laboratorio entre en operaciones, posiblemente siempre esté activo o por lo menos en horarios bien definidos, ya que es probable que los recursos a los cuales se tiene acceso a través de él, sean accedidos en cualquier momento, y esto se refiere por ejemplo al sistema de reservación del laboratorio vía Web, al calendario de prácticas, a la descarga de documentos o manuales relacionados con el laboratorio, etc.

El servidor Web debe estar única y exclusivamente dedicado al laboratorio de datos, y posiblemente deba implementar diversos servicios adicionales al de páginas Web, que presten mayor funcionalidad a la operación y administración del laboratorio. Estos servicios pueden ser:

- El acceso por medio de FIP o por HTTP a través de un navegador de hipertexto a documentación técnica referente a los equipos con los que cuenta el laboratorio, incluyendo hojas de datos y especificaciones técnicas de configuración, instalación, resolución de problemas o troubleshooting, etc. Así como a los formatos digitales de las prácticas que se hagan en el laboratorio.
- Un sistema de reservación de los servicios del laboratorio por medio de una interfaz de página Web, usando alguno de los lenguajes de programación disponibles, que sean capaces de manejar algún tipo de base de datos con la cual se pueda gestionar las reservaciones y hacer consultas. Como podría ser Java, XML, PHP, Perl, o algún otro, dependiendo de lo que necesitemos. La decisión del tipo de lenguaje utilizado es una decisión que se tendrá que tomar más adelante en función de las características estudiadas de cada uno y de lo que necesitemos, y de quién y cómo escribe el código.
- Servicio de nombres. Dentro de la red interna del laboratorio es conveniente que los equipos ya sea terminales, servidores o enrutadores sean identificados por un nombre significativo en vez de solo hacerlo a través de su dirección IP. Aunque no es necesario, tal vez sea conveniente tener el servicio de traducción de nombre a direcciones IP y viceversa.

---

El servidor Web puede implementarse por ejemplo bajo un ambiente Linux, el cual es software de libre distribución, y que además cuenta con una gran cantidad de herramientas para el trabajo en redes, desde pilas de casi cualquier protocolo hasta las más diversas herramientas de monitoreo para el desempeño del sistema. Y por otro lado es un sistema muy estable y económico, por lo que es una opción a analizar.

El hardware requerido para dicho servidor no es muy exigente, ya que se prevé que la cantidad de usuarios, servicios que satisfacer y por tanto la cantidad de procesamiento requerida para su correcta operación no es muy grande. Solo se requeriría que forzosamente contara con una NIC o interfaz adecuada para conectarse a la red.

El hablar de las especificaciones mínimas de dicho equipo para que tenga un buen desempeño, no es tan relevante para el diseño lógico y físico de la red, y por tanto serán cubiertas en el momento de implementación.

Otro aspecto a contemplar es el de la manera en que el servidor deberá estar conectado tanto a la red interna, como a Internet, ya que si se desea que pueda hacerse uso del mismo por vía remota y que las páginas Web estén disponibles en la red mundial debe realizarse un diseño tanto lógico como físico para ello.

El tema de la conexión a la red de Internet será analizado con más detalle en el capítulo siguiente, pero es importante desde ahora visualizar que debe considerarse como un tema de gran importancia.

En cuanto a otros aspectos del diseño y la operación del servidor Web que hay que considerar son los siguientes:

- Diseño del sitio Web.

El diseño del sitio Web es un tema que puede ser bastante amplio si se quiere especificar toda la información que se requiere para hacerlo.

Se deben considerar aspectos muy diversos como la configuración del sistema operativo para que pueda trabajar adecuadamente dentro de la red, se deben habilitar los servicios que brindará, se debe configurar un esquema de seguridad para evitar posibles irrupciones, se deben adecuar las herramientas para que pueda hacer un monitoreo de la actividad que haya en la red y en el mismo servidor, etc. Todo ello en función de que tanta funcionalidad necesitamos que tenga dicho servidor.

- Documentación del sitio Web.

Es necesario que se realice una buena documentación de la manera en que se configuró el servidor y de los servicios que se puede proporcionar, ya que una vez implementado y en marcha el laboratorio, cuando existan problemas con la operación del mismo sea fácil revisar la documentación y poder analizar el sistema completo con mayores probabilidades de éxito de encontrar la falla.

Asimismo estudiando esta documentación, se puede buscar la manera de optimizar de alguna forma lo ya existente, así como tener mayor facilidad cuando sea necesario actualizar algún componente.

- Costo de implementación, operación y mantenimiento.

Siendo diferente el objetivo primordial y el tema hacia el cual está orientada esta tesis, se puede considerar un tema algo apartado el diseño del contenido del servidor Web, por lo que posiblemente se requiera que un programador o alguien con los conocimientos necesarios diseñe, cree y administre el servidor de páginas Web. La tarea de configuración y elaboración del contenido Web que tenga el servidor puede posiblemente ser desarrollado por algún tercero, aunque no se excluye que se pueda hacer como parte de este proyecto, pero iría más allá de los alcances pretendidos del proyecto de esta tesis.



---

La implementación del servidor implica tanto poseer el equipo adecuado, como el tener solidamente configurado el sistema, y cada uno de estos aspectos implica que una vez instalado el laboratorio sea necesario contar con el personal adecuado para poder mantener trabajando el laboratorio.

El tipo de software y sistema operativo utilizado es también un factor en el costo asociado a la implementación del servidor, y en ese sentido se tienen dos alternativas; la primera es usar software comercial, ya sea en el sistema operativo como en las aplicaciones, con las desventajas del costo y por otro lado un dudoso soporte técnico en caso de problemas, además de que se tendría que lidiar con obligaciones de licencias y demás.

En este caso el hacer uso de software de libre distribución, con el que no se tendría problemas de licencias y costo elevado de instalación, pero con la desventaja de tener que estar más capacitado para hacer uso de él para configurar y resolver problemas.

Por otro lado también existe gran variedad de aplicaciones y herramientas para el trabajo de redes y la libertad de poder experimentar diversas opciones.

### **9.6 Equipo y material didáctico.**

En la categoría de equipo y material didáctico se puede establecer que es aquel que de alguna manera apoya en la tarea de aprendizaje de los conocimientos, procedimientos y tareas a realizar con lo que respecta a la teoría y práctica de las redes de datos.

Se puede tener como material didáctico desde equipo físico complementario hasta software que pueda realizar simulaciones de una red de datos.

En lo que se refiere a equipo adicional se pueden incluir proyectores, pizarrones blancos y los aditamentos complementarios para ellos, como pantallas blancas, apuntadores, marcadores, borradores, etc.

Estos equipos son necesarios para poder hacer la introducción, desarrollo y manejo de la clase, ya que permite tener más elementos a través de los cuáles se pueden transmitir los conocimientos y las instrucciones de parte del que imparte la clase al grupo.

Entre el software se podrían incluir herramientas como analizadores de protocolos específicos, monitores de uso de aplicaciones, sniffers, etc. Los cuales permiten el monitoreo de los protocolos que están circulando en la red, del desempeño de la misma, y detección de fallas. Dichas herramientas pueden estar disponibles tanto en forma de software comercial como en forma de freeware o shareware, o incluso bajo licencias públicas como la GNU, todo depende del sistema operativo usado en las terminales de acceso y en el servidor.

Este tipo de herramientas lógicas al ser utilizadas correctamente pueden ser muy ilustrativas de lo que está pasando en la red, por lo que se puede considerar una buena idea hacer una buena selección de las que están disponibles de diversas fuentes, para ser usadas en el laboratorio.

### **9.7 Equipamiento tentativo del laboratorio.**

En esta parte se da una lista que contiene los equipos con los que se va a contar para poder implementar el laboratorio de la Facultad de Ingeniería.

El equipamiento del laboratorio en cuanto a equipos de comunicaciones se refiere aun no está bien definido, por lo que solo se tiene una idea de cuales serán los equipos con los que se contará, entre los que se incluyen los siguientes:

Cantidad	Descripción del equipo.
10	Fraccionador RAD Mod. FCD-2
1	Switch WS-C1400(CDDI/FDDI)
1	Bridge STS-10x
5	Access Server Cisco 500-CS
2	Bridge Cisco WS-C1201
3	Enrutador Cisco AGS+
12	Enrutador Cisco 3000
5	Enrutador Cisco 4000
1	Tarjeta NP-1E para enrutador Cisco 4000
1	Tarjeta NP-1RU para enrutador Cisco 4000
1	Tarjeta NP-1RV para enrutador Cisco 4000
4	Tarjeta NP-2E para enrutador Cisco 4000
7	Tarjeta NP-4T para enrutador Cisco 4000
5	Enrutadores Cisco 7000
10	Fuente de poder 7000 CA para enrutador Cisco 7000
5	Tarjeta EIP6 para enrutador Cisco 7000
11	Tarjeta FSIP8 para enrutador Cisco 7000
5	Tarjeta RP para enrutador Cisco 7000
5	Tarjeta SP para enrutador Cisco 7000
1	Tarjeta TR2 para enrutador Cisco 7000
1	Tarjeta TR4 para enrutador Cisco 7000

Tabla 9.7.1 Equipos tentativos para el laboratorio.

Esta lista no es definitiva y puede sufrir modificaciones, pero es lo suficientemente concreta para poder realizar un proyecto en cuanto a la distribución del laboratorio.

Las terminales de acceso no están incluidas en la lista anterior y son equipos que deberán ser proporcionados según las características descritas en el capítulo dedicado a tal fin. Los detalles de operación se describirán más adelante en otro apartado debido a que están más enfocadas a la parte lógica que a la física.

El servidor Web es un tema aparte, que se sugiere se implemente para darle más funcionalidad al laboratorio, pero que debe realizarse por un tercero que pueda realizar las tareas de programación e implementación cuando el laboratorio este completamente instalado y en operación, sólo es necesario que se sigan los lineamientos dados en el capítulo correspondiente a fin de que se integre con los demás servicios del laboratorio.

### 9.8 Resumen.

En este capítulo se da una visión general introductoria de los sistemas de comunicaciones y demás dispositivos, que integrarán en sí la parte importante del laboratorio de datos.

Se habló de las funciones principales que realizarán cada uno de estos componentes y la manera en que coexistirán dentro de la red del laboratorio.

Generalmente los equipos de comunicaciones que se instalan en una red se eligen en función de los servicios y aplicaciones que se necesitan en una red de acuerdo a las necesidades de determinada empresa o institución.

Sin embargo, para el laboratorio se contará con equipos predefinidos de diversa naturaleza que en conjunto podrán suplir diversas necesidades a cubrir en las prácticas que simulen redes de datos reales, siendo

---

importante conocer bien los equipos con los que se va a trabajar para poder configurarlos y aprovecharlos al máximo en todas sus capacidades y usar todas sus funciones.

Un componente que proveerá funcionalidades adicionales a los servicios que prestará el laboratorio es el servidor WWW, a través del cual se podrán tener acceso a paginas Web que contendrán información útil al respecto de la materia, así como la facilidad de automatizar procesos como la reservación del laboratorio y otros servicios más que se podrán ir agregando conforme se crea necesario que existan.

A partir de este punto el diseño del laboratorio se enfoca en dos direcciones, que a su vez son complementarias, una es el diseño físico de la red y otro el diseño lógico. Teniendo en cuenta que aún se ve desde el punto de vista ideal, se empieza a considerar los recursos con los que se planea contar.

---

## Capítulo 10.

### Conexión local del laboratorio y conexión a Internet

#### 10.1 Introducción.

En este capítulo se considera el aspecto de conexión de la red local del laboratorio con Internet, así como los aspectos de seguridad del mismo con respecto a dicha conexión.

Para poder decidir cuál va a ser el esquema de conexión a Internet, es necesario que tengamos conocimiento de:

- Concepto de Internet.
- Los servicios que se pretenden prestar a través de él y;
- Las diferentes maneras que existen para poder realizar la conexión, asimismo de los riesgos que esto conlleva para poder crear un esquema de seguridad apropiado.

El Internet es el mayor conjunto que existe de información, personas, computadoras y software funcionando de forma cooperativa, publicando y organizando información, e interactuando en el ámbito global. Internet se presenta como un vasto almacén de información.

La conexión a Internet para nosotros tiene dos puntos de interés, el primero es que el funcionamiento de Internet es un tópico íntimamente relacionado con las redes de datos, que es la parte constitutiva del laboratorio que vamos a implementar. El segundo punto es que, los servicios que provee Internet darán más funcionalidad y capacidades al laboratorio mismo, por lo que la conexión a Internet con fines educativos se justificaría además por las prestaciones y servicios que nos va a dar.

#### 10.2 Servicios más comunes sobre Internet.

Los servicios que Internet provee son variados. A continuación se da una descripción breve de los más importantes.

- Correo electrónico.

El correo electrónico (e-mail) es de los servicios más usados de Internet. Cada persona que está conectada cuenta con un "buzón electrónico" personal, simbolizado en una dirección de correo.

El buzón de correo electrónico sirve para intercambiar mensajes con otros usuarios, y por eso no hay nunca dos direcciones iguales. La primera parte de una dirección identifica habitualmente a la persona o usuario y la segunda a la empresa u organización para la que trabaja, o en su caso al proveedor de Internet a través del que recibe la información.

El correo electrónico permite enviar texto o archivos, generalmente de tamaño pequeño. Se pueden enviar mensajes a varias personas, responderlos de forma automática, guardar directorios personales de direcciones y de grupos de colaboradores.

- World Wide Web.

La WWW es tal vez el servicio más conocido de Internet y hoy en día el más usado junto con el correo electrónico, aunque también es de los más recientes.

La WWW puede definirse básicamente como tres cosas: hipertexto, que es un sistema de enlaces que permite saltar de un lugar a otro; multimedia, que hace referencia al tipo de contenidos que puede manejar (texto, gráficos, video, sonido y otros) e Internet, sobre el que se transmite la información.

El aspecto exterior de la WWW son las páginas Web. Las páginas de la WWW están situadas en servidores Web de todo el mundo, y se accede a ellas mediante un programa denominado navegador o "browser". Este programa emplea HTML como el lenguaje que se encarga de gestionar el aspecto de las páginas y los enlaces. Una ventana muestra al usuario la información que desea, en forma de texto y gráficos, con los enlaces marcados en diferente color y subrayados. Haciendo un clic con el ratón se puede saltar a otra página,

---

que tal vez esté instalada en un servidor al otro lado del mundo. El usuario también puede navegar pulsando sobre las imágenes o botones que formen parte del diseño de la página.

Cada página Web tiene una dirección única en Internet, denominada URL. Una dirección URL indica la ubicación y el tipo de documento, el de las páginas hipertexto de la WWW comienza siempre por http, que indica el protocolo nativo usado para el transporte de los datos, aunque puede ser también ftp o https.

Cada vez son más las empresas que publican información en la Web. Y encontrarla es también cada vez más fácil. Pocas son las empresas de gran tamaño que no tienen su propia página Web hoy en día.

Parte de la gran potencia de la Web también proviene del hecho de que cada vez es más fácil publicar material, y no sólo acceder a lo que ya está allí. Existen programas gratuitos y comerciales para crear páginas HTML para la Web (similares a los programas de autoedición, sin necesidad de programación), y alquilar espacio en un servidor al que enviar las páginas es cada vez más barato y accesible. Hoy en día, cualquiera puede publicar lo que desee.

Dentro de la WWW hay servicios como los buscadores, los cuáles a través de motores de búsqueda organizan y categorizan la información de Internet. Unos organizan todos los recursos de Internet, en categorías como páginas Web, grupos de noticias, etc. Otros, mantienen índices de todo lo que se publica en la Web, y permiten buscar información por palabras y por contexto.

La Web, al facilitar la búsqueda de información, ha hecho que otros servicios de Internet como Gopher, Archie o WAIS se usen cada vez menos.

- Grupos de noticias.

Los grupos de noticias o de discusión (también llamados Newsgroups o Usenet) consisten en la publicación de mensajes en áreas específicas diferenciadas por el tema a discutir, es un sistema de conferencia y discusión de alcance global. Hoy en día existen varios miles de grupos de discusión distintos con una variedad de tópicos enorme. Hasta la llegada de la WWW los grupos de discusión (Newsgroups) eran el área más popular de Internet.

Para ver el contenido de un grupo de noticias es necesario estar suscrito al mismo y tener software visor instalado para poder verlos.

- FTP (File Transfer Protocol.)

FTP es un protocolo de transmisión de archivos que permite enviar y recibir múltiples archivos de cualquier tamaño de un lugar a otro de Internet, de modo más rápido y eficaz que mediante correo electrónico.

En Internet existen servidores FTP con programas de distribución pública, imágenes y sonidos, de libre acceso. Muchos fabricantes los usan para mantener al día a sus clientes en cuanto a nuevas versiones del software, actualizaciones o controladores. Los servidores FTP también se emplean para la distribución de software de demostración, revistas electrónicas y otros materiales.

Los servidores FTP pueden ser privados o públicos. Se accede a ellos mediante un URL o su dirección IP.

El acceso a servidores FTP puede ser tanto anónimo o con una cuenta hecha especialmente para cada usuario.

- Otros servicios.

Existen otros servicios de Internet no tan conocidos ni populares que siguen existiendo por razones prácticas e históricas. Algunos de ellos son:

**Telnet.**

Sirve para conectarse a un host remoto desde una host local. A fin de poder trabajar con ese equipo como si estuviera sentado frente a un terminal local, aunque se encuentre en la otra punta del mundo. Sin embargo por sus deficiencias de seguridad está siendo reemplazado por ssh.

**Gopher, Archie, Verónica y WAIS.**

---

Son básicamente entornos de menú y búsqueda para navegar por servidores de FTP, que mantienen bases de datos de archivos de la red que se puede consultar. Suelen incluir más información de la que se obtiene al hacer un FTP convencional, y algunos permiten consultar bases de datos.

Listas de correo.

Son servicios de mensajería entre grupos de personas, mantenidas mediante un sistema automático de correo electrónico y suscripciones gratuitas. Hay miles de listas de correo sobre temas específicos y aficiones, en grupos que varían entre pocas personas y varias decenas de miles. Pueden ser moderadas o no-moderadas, y a veces ofrecen una mejor aproximación a los debates que Usenet.

Después de haber mencionado los principales servicios de Internet, es necesario definir cuáles son los servicios que son apropiados y útiles para ser prestados por nuestro laboratorio. Cada servicio tiene una función específica que debe de ser valorada como útil o no antes de definir si se va a proporcionar. En este momento se puede considerar que los servicios que probablemente se van a proporcionar son: FTP, WWW, Telnet y correo electrónico. Sin embargo a estos pueden ser agregados otros cuando se avance en el desarrollo de este proyecto. Por ahora no es importante definir todos, ya que la infraestructura y protocolos (TCP/IP) en los que operan son los mismos, pero deberán ser estudiados en el momento de elaborar el esquema de seguridad básico de la red del laboratorio para evitar hoyos en la seguridad del mismo.

### 10.3 Tipos de conexión

Para conectarnos Internet existen varias formas de hacerlo:

- Acceso dedicado.

El acceso dedicado como su nombre lo dice, conecta la red a Internet de forma permanente, es decir las 24 horas del día durante todo el año. Este tipo de acceso es en general el mejor si se quiere y se necesita tener presencia continua, como es el caso de empresas o instituciones que proporcionan servicios a través de Internet. Por sus características implica un costo de operación y mantenimiento mayor ya que se requiere rentar un enlace dedicado (leased line) para estar conectado.

- Acceso conmutado.

Este tipo de acceso se realiza a través de líneas conmutadas, como son las líneas telefónicas de la RTPC, o de ISDN. Para poder conectarse es necesario hacer una llamada previa y autenticarse antes de poder hacer uso de la red.

ISDN es otro tipo de conexión conmutada, el servicio básico o BRI (Basic Rate Interface) proporciona dos canales B de 64 Kbps y un canal D de control.

ISDN puede dar servicio a varios usuarios pero es necesario establecer aún una conexión cada que se accede a Internet. Las tarifas de ISDN se basan en una renta y en el tiempo de conexión, por lo que si el tiempo es grande los costos se disparan.

En el acceso conmutado realizado a través de marcado, el usuario solo se conecta a la red del ISP cuando lo necesita, a través de una llamada telefónica. El costo está en función de varios factores pactados con el ISP como las llamadas realizadas, el tiempo de conexión, la cantidad de datos transmitidos, etc. más un cobro tarifario por renta mensual o anual.

Por sus características es recomendable para usuarios o empresas que no requieran presencia continua en Internet.

Tanto para la conexión dedicada como para la de marcado, el ancho de banda contratado puede ser desde el básico de 56 Kbps, hasta fracciones y múltiplos de T1's y E1's.

Para proporcionar el ancho de banda requerido se necesita usar tanto en la central como en el site del usuario, equipos de variadas tecnologías que van desde módems analógicos hasta módems digitales empleando tecnologías como SDH, ISDN, xDSL, etc. De las cuales cada una tiene sus respectivas ventajas y desventajas.

---

El tipo de acceso tradicionalmente ha sido hecho con tecnologías alámbricas pero también se puede hacer con tecnologías inalámbricas.

Este tipo de conexión tiene la desventaja de que si se requiere prestar servicios a Internet, es necesario estar conectado todo el tiempo, lo cual es muy costoso.

Para el caso particular de la conexión del laboratorio al Internet se tienen dos alternativas; la primera es a través de un ISP y la segunda a través de otra red ya conectada a Internet. Ambas opciones se explican más a detalle a continuación.

- **Acceso a Internet a través de un ISP (Internet Service Provider.)**

La conexión a Internet se puede hacer a través de un ISP (Internet Service Provider), un ISP es una empresa que establece la conexión entre un usuario e Internet, ya sea de forma dedicada o de forma temporal a través de marcado.

El servicio de conexión a Internet puede ser realizado por las empresas telefónicas o por empresas que a su vez le renten los servicios de transporte de datos a empresas telefónicas.

Los costos de la conexión varían de un ISP a otro, dependiendo de los servicios adicionales que provean; tales como espacio en sus servidores para almacenamiento de páginas Web y correo electrónico, el ancho de banda contratado, la tecnología usada, etc.

Cuando se hace la conexión a través de un ISP, este generalmente asigna un bloque de direcciones IP dependiendo del servicio contratado.

La asignación y administración de las direcciones IP serán tratadas mas adelante.

- **Acceso a Internet a través de otra red.**

Este esquema de conexión a Internet se realiza a través de otra red que ya tenga acceso a Internet, para ello es necesario conectarse a dicha red. Al tener acceso de esta manera se comparte el ancho de banda de salida que tiene esa red con la nuestra.

Una vez conectadas ambas redes, él o los enrutadores que funcionan como conexión de nuestra red con la otra, podrían enrutar correctamente los paquetes provenientes de nuestra red para que pasaran través de la red a la que nos conectamos y de ahí salir a Internet.

Para este tipo de acceso es necesario adecuarse a las políticas de uso de la otra red.

#### **10.4 Esquema de conexión.**

Una vez que conocemos los posibles esquemas en que nos podemos conectar a Internet, es necesario analizar las ventajas y desventajas de cada uno de ellos para poder decidir cuál es el que más nos conviene.

La conexión a través de un ISP no es la mejor opción, por los costos que representa y porque nuestra red no es independiente, sino que pertenece a una institución más grande que ya tiene definidas sus políticas de red.

El tipo de conexión a través de otra red, es el que se debe considerar como más seguro para la conexión a Internet, ya que el laboratorio de datos que estamos diseñando será parte de la Facultad de Ingeniería y a su vez de la Universidad Nacional, la cual, como institución educativa ya cuenta con una infraestructura de servicios de voz y datos y otras áreas de telecomunicaciones en las que los servicios del laboratorio deben de encajar.

En cuanto a los aspectos técnicos del esquema de conexión hay que considerar varios tópicos importantes:

##### **10.4.1 Obtención de direcciones IP.**

Debido a que deseamos tener acceso a la red de Internet, es necesario que tengamos una dirección o un grupo de direcciones IP válidas. Esto es debido a que, independientemente del esquema de direccionamiento que tengamos en la red interna en la que usaremos las direcciones que creamos más convenientes, necesitamos forzosamente de direcciones IP únicas en Internet, para que podamos tener acceso a la misma sin tener conflictos de direccionamiento y conectividad.

Es necesario saber donde podemos obtener direcciones IP para poder conectarnos a Internet, y éstas serán pedidas a la Universidad de los bloques que tiene asignados. De no ser así, hubiera sido necesario obtenerlas de los organismos mundiales que se encargan de repartir y asignar las direcciones IP u obtenerlas de un ISP.

Idealmente se requeriría un pequeño bloque de direcciones IP para los fines que ya se mencionaron, sin embargo si hay carencia de direcciones IP es posible que aún con una sola dirección IP podamos conectar varios equipos a través de diferentes métodos como por ejemplo usando NAT.

Los bloques de direcciones IP públicas que ocuparemos serán asignados por la UNAM a través de la DGSCA (Dirección General de Servicios de Computo Académico) la cual es la instancia facultada para el desarrollo y administración de la Red UNAM, con las siguientes atribuciones:

- Administrar y asignar todas las direcciones IP de la UNAM.
- Ceder o retirar la administración total o parcial de las direcciones IP de la UNAM a las dependencias universitarias, cuando lo considere conveniente.
- Representar a la Red UNAM ante los organismos reguladores de Internet en el ámbito nacional e internacional.
- Administrar todos los dominios y subdominios asignados a la UNAM y de los servidores encargados de su resolución.

Para la asignación de direcciones IP en los equipos del laboratorio, si consideramos que se tiene una cantidad grande de equipos, de los cuales cada uno tiene cierto número de interfaces que requieren una dirección IP propia, es fácil darse cuenta que la cantidad de direcciones IP necesarias no es pequeña, por lo que es conveniente usar direcciones privadas en los equipos que no requieran direcciones públicas, ya que es difícil obtener bloques grandes de estas direcciones para dárselas a todos los equipos.

Esto es porque la asignación de direcciones IP es limitada y administrada en forma rigurosa ya que son un recurso escaso. Por esta razón es necesario tener un esquema de direccionamiento mixto. Se deben usar direcciones públicas para equipos específicos, como el servidor, el enrutador de salida a Internet y los equipos usados para proteger del exterior a la red interna. Y todos los demás equipos pueden usar direcciones IP privadas que están ocultas al resto del mundo.

La RFC 1918 describe la asignación de direcciones IP para redes privadas.

Una red privada puede usar direcciones IP de los siguientes grupos:

Rango de direcciones		Equivalente a:
10.0.0.0	10.255.255.255	1 red clase A
172.16.0.0	172.31.255.255	16 redes clase B
192.168.0.0	192.168.255.255	256 redes clase C

La red que ocupe las direcciones anteriores no tiene que coordinarse con ningún registro de direcciones en Internet para usarlas mientras éstas estén ocultas e invisibles desde el exterior.

Las máquinas privadas aun pueden tener acceso a servicios externos mediante el uso de otras técnicas que se verán mas adelante.

Una estrategia posible es diseñar primero la parte privada de la red y usar el espacio de direcciones privado para todos los enlaces internos. Entonces, planificar las subredes públicas en las localizaciones necesarias y diseñar la conectividad externa.



---

Este diseño no tiene porqué ser indefinidamente fijo. Si posteriormente un grupo de una o más máquinas necesita cambiar su status (de privado a público, o viceversa), esto se puede hacer reenumerando sólo las máquinas involucradas, y cambiando la conectividad física en caso necesario. En localizaciones donde dichos cambios sean previsibles, es aconsejable configurar medios físicos separados para las subredes pública y privada, y así facilitar tales cambios. Para evitar intervenciones de importancia en la red, es aconsejable agrupar en sus propias subredes máquinas con similares necesidades de conectividad.

Si se puede diseñar un adecuado esquema de división en subredes que esté soportado por el equipamiento implicado, es aconsejable usar el espacio privado de direcciones del bloque de 24 bits (red de clase A) y diseñar un plan de direccionamiento con un buen camino de crecimiento. Si el hacer las subredes es problemático se puede usar el espacio de direcciones de los bloques de clase B o C.

Uno de los beneficios adicionales en usar direcciones privadas, es que el espacio disponible es relativamente grande y permite gran flexibilidad y escalabilidad para el diseño de cualquier red, por grande o compleja que sea, a diferencia de los bloques de direcciones IP públicos que generalmente son reducidos y poco flexibles.

Se mencionó que aun teniendo equipos con direcciones IP privadas se podía aún tener acceso a la red pública sin tener forzosamente que provocar conflictos con las direcciones públicas y privadas. Dos de esas técnicas son NAT y el servidor Proxy.

A continuación se describe la técnica de NAT. La técnica de servidor Proxy es descrita mas adelante en la sección de seguridad de la red, ya que su característica principal es la de prestar este servicio aunque puede servir también para usar direcciones privadas y ocultarlas si es que queremos conectarnos a la red pública.

NAT (Network Address Translation) es un estándar definido en la RFC 1631 que permite a una red de área local (LAN) utilizar un conjunto de direcciones IP internamente y un segundo conjunto de direcciones externamente. El dispositivo que hace la traducción NAT se sitúa en el punto de salida a Internet y realiza todas las traducciones de direcciones IP que sean necesarias. Dada esta característica, NAT proporciona funcionalidad de Firewall al ocultar las direcciones IP internas. La traducción NAT aporta mayor nivel de seguridad porque las direcciones IP de los equipos conectados a la LAN privada nunca se transmiten a Internet. El usuario puede tener varias direcciones privadas enmascaradas bajo una sola dirección proporcionada por el ISP.

En el diagrama 15.1 se ilustra un escenario donde se habilita NAT en un enrutador en la frontera de la zona, conectado a Internet a través de un enrutador regional proporcionado por un proveedor de servicios.

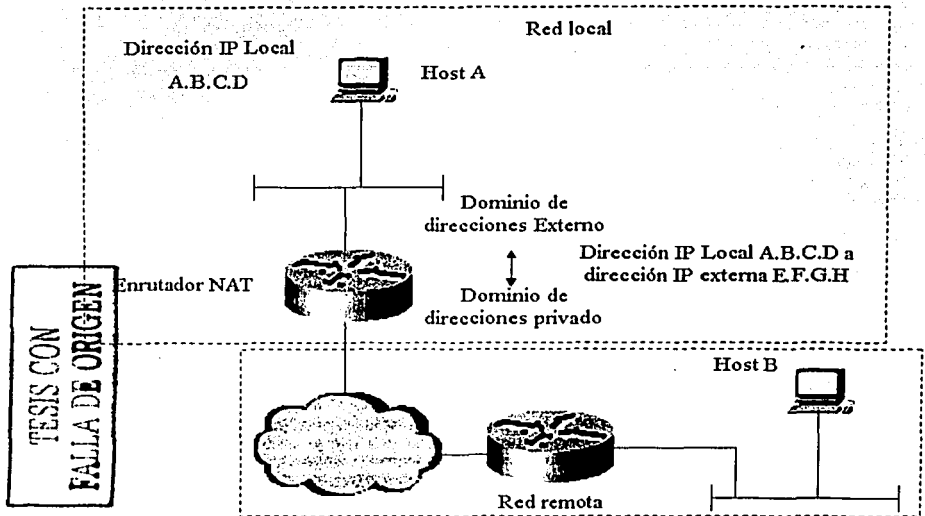


Figura 10.4.1.1: Un modelo base para ilustrar la terminología de NAT tradicional.

Existen dos variantes de NAT, el tradicional o unidireccional y el NAT bidireccional.

El NAT tradicional permitirá, en la mayoría de los casos, que las máquinas en el interior de una red privada accedan de manera transparente a máquinas en la red externa. En un NAT tradicional, las sesiones son unidireccionales, salientes desde la red privada. Esto contrasta con el NAT bidireccional, que permite sesiones en los sentidos tanto saliente como entrante.

Con el NAT bidireccional, las sesiones pueden iniciarse tanto desde máquinas en la red pública como desde máquinas en la red privada. Las direcciones de la red privada se asocian a direcciones globales únicas, estática o dinámicamente, según se establecen las conexiones en cualquier sentido.

NAT asocia direcciones en la red privada con direcciones en la red global, y viceversa, para proporcionar un enrutamiento transparente a los datagramas que atraviesen varios dominios de direcciones. En algunos casos la asociación puede extenderse a los identificadores de nivel de transporte (como los puertos TCP/UDP). La asociación de direcciones se realiza al comienzo de una sesión. A continuación se describen los dos tipos de asignaciones de direcciones.

En el caso de asignación estática de direcciones, existe un mapeo uno a uno de direcciones para las máquinas entre una dirección privada de red y una dirección externa de red durante el tiempo en funcionamiento del NAT. La asignación estática de direcciones asegura que NAT no tiene que administrar la gestión de direcciones con los flujos de sesión. En este caso, las direcciones externas son asignadas a las máquinas de la red privada, o viceversa, de manera dinámica, basándose en los requisitos de uso y el flujo de sesión que el NAT determine heurísticamente. Cuando la última de las sesiones que use una dirección asociada termine,

---

NAT liberará la asociación para que la dirección global pueda ser reciclada para su posterior uso. La naturaleza exacta de la asignación de direcciones es específica de cada implementación de NAT.

NAT es una tarea que implica cálculos intensivos incluso con la ayuda de un algoritmo inteligente para el ajuste de las sumas de verificación, puesto que cada paquete de datos implica búsquedas y modificaciones en la tabla de NAT. En consecuencia, la velocidad de reenvío del enrutador puede descender considerablemente. Sin embargo, mientras que la velocidad de proceso del dispositivo de NAT supere la necesaria para satisfacer la velocidad de línea, esto no debería suponer problema alguno.

NAT incrementa las posibilidades de direccionar erróneamente. Por ejemplo, la misma dirección local puede estar ligada a diferentes direcciones globales en diferentes momentos, y viceversa. En consecuencia, cualquier estudio del flujo de tráfico basado solamente en direcciones globales y puertos podría resultar confuso y provocar la mal interpretación de los resultados.

Si alguna máquina está abusando de Internet de alguna manera (como tratando de atacar a otra máquina, o incluso enviando grandes cantidades de correo basura o por el estilo) es más difícil averiguar el origen de los problemas porque la dirección IP de la máquina está oculta en un enrutador NAT.

Cualquiera que sea la manera de conexión a Internet, es prioritario tener un esquema de direccionamiento IP compatible con la red mundial, y adecuarnos a las limitaciones de este recurso para poder realizar la conexión del laboratorio a Internet.

#### **10.4.2 Nombre del servidor en la red y registro del dominio o subdominio.**

Par facilitar su uso, los equipos conectados a Internet están asociados con nombres que son más fáciles de recordar y más representativos que una dirección IP. Aunque no es necesario tener un nombre para poder acceder a un recurso en Internet, es una manera de facilitar la localización del mismo.

Para poder hacer uso de un nombre de dominio o de subdominio es necesario registrarlo en forma única en el mundo, de esta manera se evita ambigüedad en la conexión a dos equipos diferentes que tengan nombres iguales.

En el mundo existen varios organismos internacionales y nacionales que se encargan de administrar las bases de datos que contienen los nombres de equipos con las direcciones IP asignadas a cada uno de ellos.

Existen ciertas reglas y procedimientos técnicos y administrativos que seguir para poder concluir el proceso de asignar un nombre a un servidor de Web, FTP, correo electrónico, etc. En nuestro caso la asignación de nombres será bajo un esquema de subdominio del dominio de la UNAM, dicho registro será hecho por la DGSCA que es la encargada de tales tareas dentro de la UNAM.

#### **10.4.3 Conexión del servidor Web a la red y seguridad del mismo.**

El servidor Web debe de ser accesible para alguien que esté en el interior de nuestra red y también para los que estén afuera, por lo que es un recurso que está siempre visible y por tanto predispuesto a problemas de seguridad.

La seguridad del servidor es un tema muy importante a considerar desde el diseño inicial, ya que busca evitar que los servicios y los recursos a los que se accede sean denegados, dañados o destruidos por cualquier medio. La seguridad de la red se considera más a fondo en otro apartado.

Al final de este capítulo se sugieren varios esquemas de conexión en las que se integra la red interna con la red externa.

#### **10.4.4 Acceso a los servicios brindados.**

Este es un aspecto que tiene que ver mucho con el aspecto de seguridad, se deben de planear en conjunto para poder tener un esquema coherente de dichos servicios.

Esto es con el fin de ofrecer facilidad de uso y por otro lado el de proteger estos recursos de ataques que limiten o atrofien dichos servicios.

#### **10.4.5 Monitoreo de la actividad de la red y en el servidor.**

---

Parte de la estrategia de seguridad de la red tiene que ver en el cómo se van a monitorear los eventos que tengan lugar dentro de la red. En nuestro caso se puede hacer a través de un servidor Proxy. Esta alternativa es analizada y propuesta mas adelante.

### **10.5 Esquema de seguridad.**

Se debe hacer un balance costo-beneficio para saber qué soluciones se deben usar par proteger la red y sus recursos. En nuestro caso hay que analizar uno por uno los dispositivos, servicios y recursos que están en juego. En lo que respecta al acceso a Internet por parte de la red interna se considera que no debe de estar restringido, es decir que se debe de tener acceso a servicios como WWW, FTP, e-mail, etc. aunque aun deben de estar sujeta a las normas y políticas de uso y divulgación de la información estipuladas por el reglamento del laboratorio. Sin embargo el acceso desde la red exterior hacia la red interna debe de ser vigilado, por las siguientes razones:

- Las únicas fuentes de información públicas disponibles estarán en el servidor.
- El acceso a los equipos terminales de la red interna debe de ser permitido en situaciones especiales pero de forma expresa y temporal.
- El acceso a los equipos de comunicaciones, es decir los enrutadores y switches. Normalmente éstos están ocultos en redes privadas. Sin embargo, si planteamos como uno de los objetivos del laboratorio el permitir el uso de los mismos para realizar prácticas por vía remota es entonces necesario permitir dicho acceso.

Este último es el problema de seguridad más importante que resolver. Se debe pensar que si no se pone una barrera que filtre el acceso no autorizado a los equipos, éstos por si mismos no cuentan con mecanismos de seguridad y registros de actividad avanzados y seguros.

Por este motivo es necesario filtrar el acceso a los equipos para que solo los usuarios autorizados puedan hacerlo y de cualquier manera su actividad sea registrada.

Nos referimos a usuarios autorizados a aquellos que según ciertas reglas puedan considerarse como tales. Entre estas reglas se pueden tener las siguientes:

- La primera y la realmente esencial, es al de tener una cuenta de usuario válida. Si no se definen mas reglas, éste sería el único requisito para tener acceso a los equipos seleccionados para ello. Por eso hay que tener un buen control de tales cuentas, mediante una asignación y caducidad determinadas por el procedimiento administrativo del reglamento de laboratorio, el cual será tratado por otro capítulo. Las cuentas pueden tener privilegios que van desde los de solo lectura y monitoreo, a cuentas privilegiadas con las cuales es posible modificar la operación y configuración de los equipos de comunicaciones.
- Otra regla para incrementar la seguridad en el uso de los equipos, es la de crear listas de acceso con las cuales se asegura que los equipos sólo sean accedidos desde direcciones IP permitidas. Esto evita que cuentas válidas puedan ser usadas por alguien que de alguna manera se hizo de alguna de ellas, ya que Telnet por ejemplo envía sus comandos (entre ellos username y password) en texto plano y cualquiera que esté "escuchando" el tráfico Telnet con un Sniffer puede verlo y apropiárselo y luego usarlo desde cualquier lugar. Aunque este caso se puede evitar usando SSH; es una muestra de lo que puede suceder si se quiere apropiarse de cuentas usadas para la autenticación en los equipos.

Existen varias estrategias para poder generar un esquema de seguridad, pero el objetivo principal es el de proteger los recursos y servicios del laboratorio y mantenerlos intactos y lo menos vulnerables posible ante ataques tales como: denegación de servicio (DoS), congestión en la red, tormentas de broadcast, etc. Los cuales afectan en mayor o en menor medida el funcionamiento del laboratorio.

Antes de conocer y decidimos por alguna de estas estrategias es necesario saber de que tipo de eventos nos debemos proteger a fin de saber cual es el mejor método para evitarlo.

Una amenaza es un peligro potencial que puede romper las medidas de seguridad informática que tenemos establecidas. Entre ellas hay dos tipos:

- 
- **Accidentales:** No son premeditadas y en ellas podemos incluir los posibles fallos del hardware y software de nuestra instalación.
  - **Intencionadas:** Por medio de algo o de alguien se produce un ataque a nuestra infraestructura e información, o el uso de recursos por parte de alguien no autorizado o para fines distintos de los que fueron creados.

Nos centraremos por razones obvias en las amenazas intencionadas, de las cuáles las más importantes son:

- **Divulgación no autorizada de la información.**

Consiste en que la información en la red que no es de uso público, sea divulgada o extraída, dicha información puede ser confidencial o de uso restringido y por lo tanto debe de reducirse el riesgo de ser difundida, ya sea por alguien desde la misma red interna o por alguien que desde el exterior la saque.

- **Modificación no autorizada de la información.**

Este es el siguiente riesgo que la información puede tener, ya que aunque no sea privada o confidencial, el modificar la información pública, por ejemplo en la página Web de una empresa, da una mala imagen de la empresa que representa.

- **Enmascaramiento (spoofing.)**

Es una técnica en la que un equipo finge ser otro que se considera confiable para ciertos equipos usando la dirección IP del equipo confiable original. Lo cual al lograrse pone al equipo impostor con los mismo privilegios que el equipo original.

- **Acceso no autorizado a recursos.**

Este es el uso y/o acceso a los recursos de la red, tales como el ancho de banda, información privilegiada, uso de dispositivos o servicios por parte de alguien que no esta autorizado a hacerlo.

- **Denegación del servicio.**

Este es un ataque que puede ocasionar que los verdaderos usuarios de la red no puedan hacer uso de sus recursos, ya que estos se negarán. Puede ser causado por alguien que sature la red, modifique cuentas, apapare recursos, etc.

Entre los dispositivos que se utilizan para prevenir y tratar de proteger las redes privadas, se encuentran los Firewalls y los servidores Proxy.

### 10.5.1 Firewall.

Un Firewall es un sistema o conjunto de sistemas que crean una barrera con fines de seguridad entre dos redes, el propósito de una red con Firewall es mantener a intrusos fuera del alcance de los recursos e información confidencial que se encuentran dentro de una red susceptible a ataques.

Un Firewall filtra el tráfico que está cruzando de un lado a otro de las redes.

Generalmente los Firewalls están configurados para prevenir el acceso no autorizado desde el exterior, esto previene actos de vandalismo, en máquinas y software de la red.

Según las políticas de seguridad que se definan, es necesario bloquear el paso de cierto tipo de servicios a través de los cuales se sabe que hay más posibilidades de sufrir un ataque.

Existen Firewalls más elaborados que bloquean el tráfico de afuera para adentro, permitiendo a los usuarios del interior comunicarse libremente con la red exterior.

Las redes Firewall pueden proteger de cualquier tipo de ataque externo a la red, siempre y cuando se configuren para ello.

Para que un Firewall tenga una efectividad completa, debe ser una parte consistente en la arquitectura de la red, ya que debe ser el único camino por el cual deban pasar los datos para poder proteger a la red completa, esto es, que aunque se tenga un Firewall muy bien configurado, pero en algún punto de la red hay algún acceso sin proteger, de nada serviría tener el Firewall, un ejemplo de este tipo de puntos de acceso es por ejemplo vía telefónica a través de módem.

Por otro lado, el Firewall no nos puede proteger de ataques que tengan su origen en el interior de la red, así como tampoco de usuarios malintencionados o mal capacitados, por lo que una parte importante en la seguridad de la red es tener una adecuada política de uso dentro de la misma. De igual manera, tampoco nos

---

puede proteger de virus, ya que el mecanismo a través del cual éstos pueden dañar los recursos de la red es diferente y fuera del alcance de los dispositivos de red.

Hay que reconocer algunas decisiones básicas que tomar al momento de tener que diseñar e implementar un Firewall para una red.

- De qué manera se va a reflejar la política del laboratorio con la que se operará el laboratorio, esto se refiere, al si se va a destinar el Firewall para denegar todos los servicios, excepto aquellos críticos para la misión de conectarse a la red o si este se destina para proporcionar un método de medición y auditoría de los accesos no autorizados a la red.
- También se requiere analizar que nivel de vigilancia, redundancia y control se quiere. Y finalmente el aspecto financiero. El precio del sistema más sofisticado es realmente muy elevado, y debe hacerse una valoración, de qué es lo que se está obteniendo y si lo vale, por lo que hay que evaluar a conciencia, qué es lo que se pone en riesgo en la red y las medidas que serían necesarias para protegerlo, y de esta manera saber qué nivel de protección se justifica en la red y por tanto el costo asociado a ello.
- En cuanto al asunto técnico, se debe tomar la decisión de colocar una máquina desprotegida en el exterior de la red para correr servicios Proxy tales como Telnet, FTP, etc., o bien colocar un enrutador a modo de filtro, que permita comunicaciones con una o más máquinas internas. Hay sus ventajas e inconvenientes en ambas opciones, con una máquina Proxy se proporciona un gran nivel de auditoría y seguridad en cambio se incrementan los costos de configuración y se decreta el nivel de servicio que pueden proporcionar.

En primer lugar vamos a describir el sistema de Firewall, ya que es la primera opción para proteger la red.

Conceptualmente, hay dos tipos de Firewalls:

- Firewall de nivel de red.
- Firewall de nivel de aplicación.

Entre estos dos tipos de Firewalls no hay tantas diferencias, las últimas tecnologías no aportan claridad para distinguirlos hasta el punto que no está claro cuál es mejor. Pero en cualquier caso, se deberá prestar atención y poner mucho cuidado a la hora de instalar el que realmente se necesita de acuerdo a los requerimientos de seguridad que se requieren en el laboratorio.

#### **Firewalls a nivel de red.**

Los Firewalls a nivel de red generalmente toman las decisiones basándose en la dirección IP fuente, la dirección IP de destino y puertos TCP o UDP, todo ello en paquetes individuales IP. Un simple enrutador con estas capacidades es un Firewall tradicional a nivel de red.

Los Firewall a nivel de red modernos se han sofisticado ampliamente, y ahora mantienen información interna sobre el estado de las conexiones que están pasando a través de ellos, los contenidos de algunos datagramas y otras cosas. Un aspecto importante que distingue a los Firewall a nivel de red es que enrutan el tráfico directamente a través de ellos. Los Firewalls a nivel de red en la actualidad tienden a ser más veloces y más transparentes a los usuarios.

#### **Firewalls a nivel de aplicación**

Son generalmente hosts que corren bajo servidores Proxy, que no permiten tráfico directo entre redes y que registran toda la actividad implicada en cada conexión y auditan el tráfico que pasa a través de ellos. Los Firewall a nivel de aplicación se pueden usar como traductores de direcciones de red, desde que el tráfico entra por un extremo hasta que sale por el otro. Los primeros Firewalls a nivel de aplicación eran poco transparentes a los usuarios finales, pero los modernos Firewalls a nivel de aplicación son bastante transparentes. Los Firewalls a nivel de aplicación, tienden a proporcionar mayor detalle en los informes auditados e implementan modelos de conservación de la seguridad. Esto les hace diferenciarse de los Firewalls a nivel de red.

Se puede resumir que los Firewall tienen dos funciones principales, la primera se asegura que nadie desde el exterior puede acceder a recursos de un equipo perteneciente a la red. Con ello se evita que, por falta de prudencia o de pericia al configurar un equipo, un extraño sea capaz de entrar en la red y/o acceder a recursos, archivos compartidos o impresoras de red.

Con la segunda función es posible configurar de forma selectiva direcciones IP, así como puertos, que están disponibles para entrada y/o salida de datos. Gracias a esta función podremos inhibir el acceso a ciertas direcciones, o impedir que los mensajes provenientes de un determinado servidor lleguen a nuestra red.

Una de las funciones más básicas de un Firewall es la de filtrar paquetes. La parte de filtrado de paquetes examina las direcciones IP (así como los puertos de E/S) de procedencia y destino de cada paquete, examinando su cabecera. Mediante una serie de reglas, denominada la lista de control de acceso, el filtro determina si acepta o rechaza los paquetes IP individuales.

En forma breve se puede decir que cada puerto es una conexión lógica que está destinada a una aplicación en específico, y si sabemos a que número de puerto va dirigido el paquete IP, se puede saber hacia qué aplicación esta dirigida y de cuál viene.

Los números de puertos TCP y UDP van desde 0 a 65536. Los puertos 0 a 1024 están reservados para el uso de ciertos servicios (Well Known ports). Por ejemplo para el servicio HTTP, el puerto definido por defecto es el 80, y no es necesario especificarlo en la URL.

El listado de puertos y sus servicios proporcionados es bastante largo, pero los más significativos son los siguientes.

Número de Puerto	Servicio	Lo que hace
15	netstat	Información sobre la red
20	FTP	Transferencia de archivos (datos)
21	FTP	Transferencia de archivos (control)
22/tcp	ssh	SSH Remote Login Protocol
23	Telnet	Conexión remota
25	smtp	Para crear e-mail.
69/tcp	tftp	Trivial File Transfer Protocol
79	finger	Información sobre los usuarios
80	http	Servidor Web
88/tcp	kerberos	Kerberos
107	rtnet	Telnet remoto
109/tcp	pop2	Post Office Protocol Version 2
110	pop3	Email entrante Version 3
115/tcp	sftp	Simple File Transfer Protocol
143/tcp	imap	Internet Message Access
161/tcp	snmp	SNMP
220/tcp	imap3	Interactive Mail Access Protocol v3
443	shhttp	servidor Web teóricamente seguro
513/tcp	rlogin	Remote login
514/tcp	shell	Shell remota
515/tcp	printer	Spooler

Tabla 10.5.1.1. Puertos UDP y TCP más conocidos.

Las reglas de filtrado permiten restringir los paquetes que provengan o se dirijan a un determinado puerto o dirección IP. En general, estas reglas se aplican para cerrar el tráfico hacia ciertos puertos y dejar abiertos sólo los realmente necesarios para los servicios que se emplean. Así, cerrando el puerto FTP de salida, puerto

---

20, se garantiza que ningún usuario externo podrá descargar (al menos bajo protocolo FTP) programas o datos del interior de la red.

### 10.5.2 Servidor Proxy.

El rol de un servidor Proxy es actuar como un enlace entre la red interna e Internet. Lo hace al permitir el acceso directo a Internet desde atrás del Firewall al abrir un socket en el host corriendo el servicio Proxy (esto bastión) y permitiendo comunicación vía ese socket para salir.

Generalmente implementados en el host bastión, los servidores Proxy son frecuentemente usados para controlar el acceso a la red interna y son muy seguros si se configuran correctamente, pero de no ser así pueden afectar el funcionamiento de la red. El servidor Proxy debe de estar configurado de manera que solo permita el acceso a los servicios requeridos y que se nieguen los otros. Es común que se instale software de servidor Proxy para servicios como Telnet, WWW o FTP conjuntamente, aunque es posible hacerlo para cualquier servicio adicional que se desee brindar.

Es posible instalar en el mismo host el servidor Proxy, el servidor Web, el servidor FTP o cualquier otro, pero no es lo más recomendable, ya que si este host deja de funcionar todos los servicios dejarían de prestarse, además si es atacado una vez pasado su esquema de seguridad todos los servicios estarían comprometidos.

Los servicios que se pretenden proporcionar deben de ser instalados en el o los servidores, los cuales deberán tener presencia continua en Internet; y deberán ser configurados adecuadamente para ser consistentes con el esquema de seguridad de la red.

Los servicios que se van a prestar se instalan de acuerdo a las plataformas y sistemas operativos en el servidor. Por ejemplo si el sistema operativo (OS) es UNIX, el servicio Web puede ser prestado por Apache, o si es Windows NT Server o Windows 2000 Server con IIS (Internet Information Server) o cualquier otro software que proporcione la funcionalidad necesaria, la seguridad del servidor y facilidad de administración.

Después de plantear las diferentes opciones típicas para implementar un esquema de seguridad en una red, es preciso definir cuales de ellas son las apropiadas para nuestro laboratorio. Para ello se deben de confrontar los pros y los contras.

Entre los pros se encuentra una mayor confianza por tener una red menos vulnerable a ataques o daños que afecten sus servicios, sus funciones o su infraestructura.

Entre los contras se puede citar la complejidad agregada en el diseño, configuración y puesta en marcha de dicho esquema, sin contar con las pruebas y el monitoreo necesarios para verificar que esté funcionando.

Otro contra es el costo asociado. Si se usan componentes de hardware, estos son caros. Si se usan soluciones basadas fundamentalmente en software pueden ser mucho más económicas si se saben elegir.

El esquema de seguridad de nuestro laboratorio al final de cuentas debe de adecuarse a los recursos disponibles.

### 10.6 Posibles esquemas de conexión.

Después de establecer los requisitos que se deben de satisfacer para integrar los equipos del laboratorio en la red interna y la red externa, tanto en el aspecto operativo como en el de seguridad, es necesario integrar un esquema de conexión y de seguridad adecuado.

La elección del esquema de seguridad y de sus componentes está en función de lo siguiente:

- Funciones que se pueden desempeñar.
- Esquema de operación.
- Esquema de conexión.
- Opciones de implementación.

A partir de estos parámetros podemos definir las ventajas y desventajas de cada uno, las cuáles se verán mas adelante cuando se propongan los esquemas en particular, tanto en conjunto como individualmente ya que en estos esquemas se integran dispositivos NAT, Proxy y enrutadores.

Se sabe que la conectividad a la red externa se realizará a través de un enrutador dedicado a tal tarea, este equipo estará conectado a la red de la Facultad de Ingeniería o a la de DGSCA directamente y por el otro lado a nuestra red interna.



Se debe de usar algún mecanismo para ocultar la red privada interna del exterior, tanto por razones de ahorro de direcciones IP públicas como por razones de seguridad. Se recomienda usar algún equipo para poder tener conectividad desde esa red privada a la red externa. Así como también proteger el servidor Web y demás servicios del exterior.

En lo que se refiere a los protocolos soportados por los equipos conectados a Internet están la pila de protocolos TCP/IP. En lo referente al protocolo o protocolos de enrutamiento usados es necesario consultarlo y acordarlo con DGSCA o el área encargada de la conectividad en la Facultad de Ingeniería para tener compatibilidad y saber cuál configurar y bajo que parámetros. Posiblemente se use algún protocolo IGP (Interior Gateway Protocol) como RIP v2, IGRP EIGRP u OSPF, o con menor probabilidad se deba usar un protocolo EGP (Exterior Gateway Protocol) como BGP 4.

En vista de las diferentes opciones para planear el diseño del laboratorio, se pensaron varios esquemas de conexión, de los cuales uno puede ser el que se implemente en el laboratorio tal como se propone o con una versión mejorada de alguno de estos esquemas, en función de los recursos con los que se cuente.

#### 10.6.1 Esquema 1. Esquema simple de conexión.

Este es el esquema de conexión más simple, y por lo tanto el más fácil de implementar. Sin embargo cuenta con muchas deficiencias en el aspecto de seguridad.

Habrà un enrutador Cisco 2500 conectado a Internet el cual va a ser el Gateway para que podamos conectar la red del laboratorio con la red exterior. Una vez dirigidos los paquetes desde el exterior hacia nuestra red, el enrutador entregará los paquetes al host destino y viceversa. Como tenemos el problema de los equipos con direccionamiento privado es necesario usar algún método para poder conectarlos a la red pública. Sin embargo si solo son algunos hosts los que requieren conectividad es posible que se coloquen en el mismo segmento en el que esté el servidor Web y puedan salir directamente a Internet.

El esquema propuesto es el mostrado en la figura siguiente.

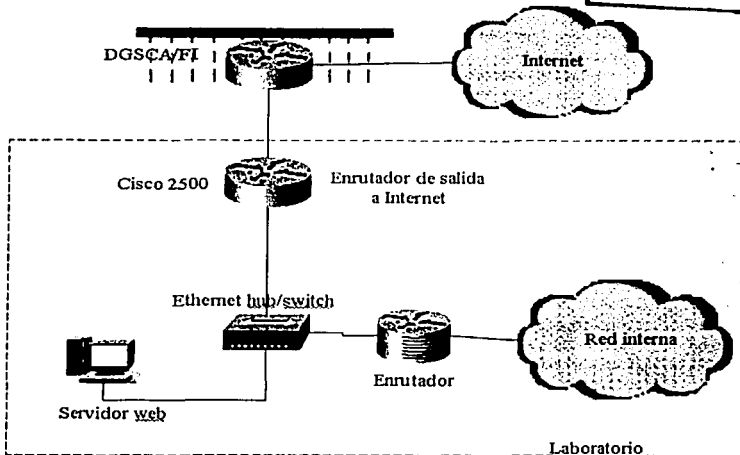


Figura 10.6.1.1

Este esquema por su simplicidad no cuenta con ningún método de seguridad implementado, salvo los que tenga cada host individualmente.

### 10.6.2 Esquema 2: Firewall a nivel de red y dispositivo NAT

Este es el segundo esquema de conexión que integra los requerimientos de conectividad, manejabilidad y seguridad del laboratorio.

El dispositivo NAT es un enrutador que es capaz de realizar la traducción de direcciones privadas a una dirección IP pública disponible. Esto requiere que el enrutador tenga la versión adecuada de IOS. La traducción NAT se necesita con el fin de poder disponer de conectividad de la red interna con Internet, sin usar un número grande de direcciones IP públicas. Esto se puede hacer a través de este método con al menos una dirección IP pública que es la de la interfaz conectada a Internet.

El Firewall a nivel de red es un enrutador capaz de filtrar los paquetes IP entrantes y salientes. Los detalles de su funcionamiento fueron dados anteriormente. El fin primordial por el cual se necesita es el de proporcionar seguridad básica a los equipos que son accesibles en nuestra red desde Internet.

A pesar de que el Firewall filtra direcciones IP selectivamente no es capaz de realizar auditoría de la actividad de la red ni funciones de seguridad más avanzadas, lo cual necesitamos para poder permitir al acceso a los equipos de comunicaciones para prácticas vía remota si es que queremos proporcionar este servicio.

El esquema propuesto es el mostrado en la figura siguiente:

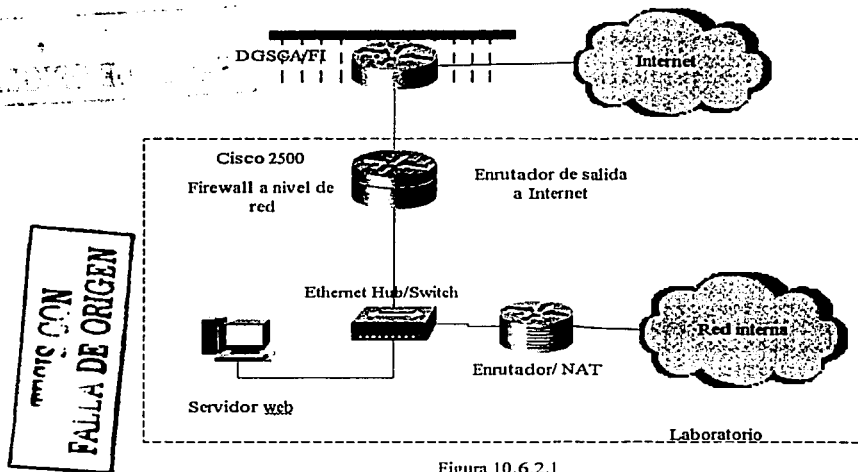


Figura 10.6.2.1

Usamos un enrutador 2500 conectado a la red de DGSCA o de la Facultad de Ingeniería a través de una interfaz serial corriendo el protocolo de enrutamiento apropiado. Debemos anunciar rutas lo más resumidas posibles, y preferentemente una sola ruta sumariada, con el fin de evitar agregar complejidad en las tablas de enrutamiento de redes externas, aunque esto dependerá del bloque de direcciones que nos sea asignado.

---

Para proporcionar la funcionalidad de Firewall es necesario configurar listas de acceso con el fin de filtrar el tráfico desde y hacia direcciones IP predefinidas.

Una interfaz Ethernet estará conectada a nuestra red de dispositivos con direcciones IP públicas como el servidor, el dispositivo NAT y otros equipos que se quisieran conectar.

El servidor Web necesita tener una dirección IP fija ya que generalmente se va a acceder a él por medio de una URL que tiene asociada una dirección IP fija, y si esta cambiara ya no sería accesible usando la URL con la IP anterior.

Desde el punto de vista de los enrutadores externos, nuestra red debe de aparecer como una entidad única, aunque internamente tengamos segmentación a través de subredes y usemos enrutadores internos para direccionar y aislar el tráfico entre subredes.

El dispositivo NAT tendría en la interfaz Ethernet configurada una dirección IP pública y en las otras interfaces direcciones IP privadas pertenecientes a la red interna privada. Para ello se necesita configurar al enrutador con una o varias direcciones IP públicas incluyendo la de la interfaz Ethernet para que puedan ser usadas para traducir las direcciones privadas de los equipos que necesiten salida a Internet, pero que por razón de no tener una dirección pública no lo podían hacer.

Con esto podemos tener el esquema de direccionamiento privado que nosotros deseamos en la red privada sin privarnos de la libertad de poder conectarnos a la red pública.

El acceso desde afuera podrá ser filtrado por direcciones, paquetes y servicios específicos permitidos en las listas de acceso del enrutador de salida a Internet. Para poder prestar servicios definidos es necesario permitir su tráfico específicamente, y denegar los otros a menos que se autoricen.

Sin embargo este esquema no proporcionaría las funciones de supervisión del acceso a la red interna mas que por el filtrado del enrutador a Internet, por lo que una vez pasado este, no habría otra protección adicional ni manera de saber la actividad de la red.

### **10.6.3 Esquema 3. Servidor Proxy y enrutador NAT.**

El tercer esquema soluciona los problemas con un método diferente. En este caso el enrutador de salida a Internet permite el paso de todos los paquetes de entrada y salida, pero solo si van dirigidos o provienen del servidor Proxy instalado en la red.

El servidor Proxy se encargará de varias tareas. La primera es que solo proporcionará los servicios que le sean configurados. En el aspecto de seguridad se podrán controlar aspectos avanzados como el monitoreo de la actividad y del tráfico en la red. La segunda es que permitirá a los equipos de la red privada conectarse usando la dirección IP del servidor Proxy, con lo que las direcciones privadas seguirán ocultas al exterior de la red.

El esquema propuesto es el mostrado en la figura siguiente.

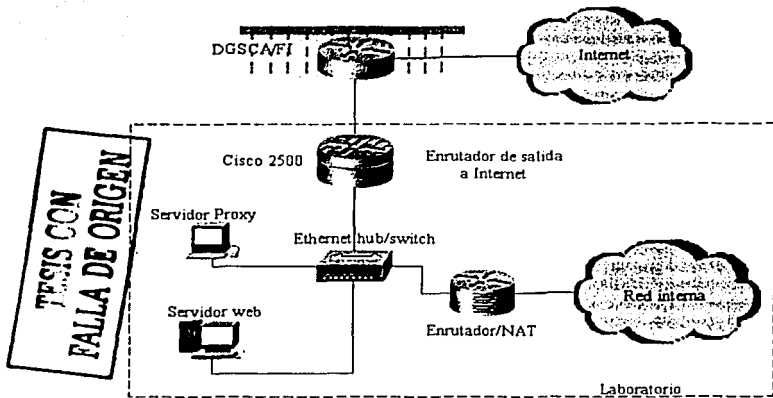


Figura 10.6.3.1

Todo el tráfico entre el interior y el exterior de nuestra red pasará por el servidor Proxy, para tal fin deben de configurarse cada uno de los equipos que pasen a través de él, tanto los de la red interna como estaciones de trabajo y equipos que quieran salir de la red, así como el enrutador que solo debe permitir el tráfico saliente y entrante a través de servidor Proxy.

Este esquema proporciona un nivel de seguridad mayor que el anterior, pero necesita que se configure adecuadamente tanto la red como el servidor Proxy. El servidor Proxy puede instalarse en una PC y cargar el software adecuado para los servicios que se pretenden prestar.

#### 10.6.4 Esquema 4. Esquema combinado.

Este es el último esquema de conexión, el cuál es una combinación de los esquemas y técnicas planteados anteriormente.

Se combina la funcionalidad del filtrado a nivel de red, y el monitoreo y auditoria del tráfico de red usando un servidor Proxy.

En el caso de las direcciones privadas aun es necesario hacer la traducción a direcciones públicas, lo cual se puede hacer con NAT o con el servidor Proxy, según se decida al final. Ya que aunque son técnicas diferentes el resultado es el mismo.

El esquema propuesto es el mostrado en la figura siguiente.

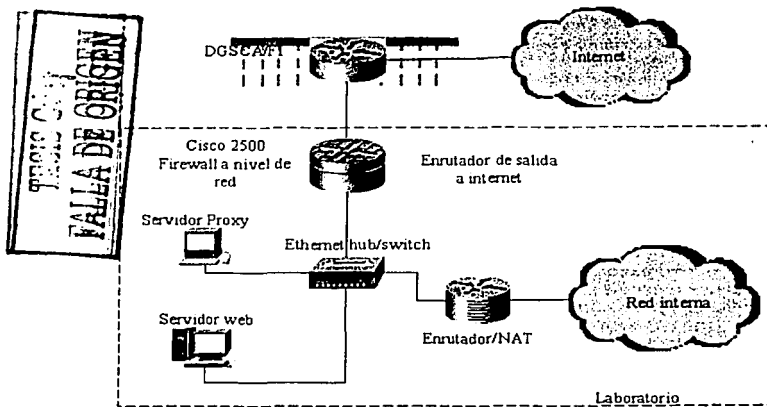


Figura 10.6.4.1

Por sus características es el más complejo y más difícil de administrar y mantener, pero es el que proporciona mayor seguridad. Sin embargo como se dijo antes debe ser necesario valorar si el trabajo de preparar e implementar un esquema de seguridad tan sofisticado es necesario.

Por otro lado aunque no sea necesario un esquema tan complejo puede ser un buen ejemplo práctico de los temas que se pudieran tratar en la teoría de los cursos que se pudieran proporcionar en la Facultad de Ingeniería.

## 10.7 Resumen.

En este capítulo se presentaron diversos esquemas con los cuales se pueden cubrir los requerimientos de conectividad y seguridad del laboratorio. Cualquiera de estos esquemas, pueden implementarse de acuerdo a casi los mismos recursos disponibles, por lo que la elección entre ellos puede hacerse en base a las necesidades de seguridad y funcionalidad deseadas.

Como se pudo ver en este capítulo el tema de la conexión a Internet y la seguridad son temas muy vastos, y sólo se pudo dar una visión general de los aspectos a cubrir, así como las posibilidades de conexión que se pueden implementar en el laboratorio con sus respectivas ventajas y desventajas. Las cuales deberán adecuarse a los recursos con los que se contará.

El esquema elegido no necesariamente es el definitivo, ya que se tiene la posibilidad de poder modificarlo ya que es fácil hacer cambios en la conectividad física y lógica del laboratorio en el caso de que en algún momento se cuente con más recursos que poner a funcionar o se requiera dar más funcionalidad a lo ya existente en el laboratorio.

Los procedimientos más detallados de cómo se pueden llevar a cabo las configuraciones necesarias son vistas en el capítulo siguiente, en el que se mencionarán los procedimientos y comandos necesarios, así como la manera de usarlos para llevar a cabo las tareas que se han mencionado en este capítulo.

## Capítulo 11. Configuraciones y conexiones Tipo.

### 11.1 Detalles técnicos de implementación.

El procedimiento de implementación de la red implica configurar muchos dispositivos, entre ellos Switches, HUBs, enrutadores, servidores, etc. La configuración de estos dispositivos requiere repetir procedimientos comunes que no es necesario detallar cada que se haga en cada uno de ellos, ya que se volvería repetitivo, por ello a continuación se presentan los procedimientos más comunes que es necesario conocer para poder implementar y configurar la red del laboratorio, simplemente siguiendo un esquema más simple de conexión en el que se establecen los parámetros principales que van a variar de equipo en equipo.

### 11.2 Configuración lógica.

En este momento ya se ha hecho referencia a varios comandos para poder configurar un equipo a través del IOS de los equipos Cisco, el cual se encarga de gestionar el funcionamiento y operación del dispositivo tal como cualquier sistema operativo.

En los puntos siguientes e detallaran los procedimientos y comandos usados comúnmente para poner en marcha el laboratorio.

#### 11.2.1 Configuración del IOS.

Para poder configurar correctamente el enrutador es necesario saber en que modo de configuración se deben introducir los comandos específicos para cada tarea, de no hacerse así los comandos no se podrán interpretar correctamente por el IOS o simplemente no serán reconocidos.

Modo de usuario normal.	Modo inicial al ingresar al enrutador, si hay un password configurado debe introducirse para acceder al enrutador. Desde este modo solo se puede monitorear información general del enrutador. Se tiene el prompt: <i>NombreEnrutador&gt;</i>
Modo de usuario privilegiado.	Del modo de configuración de usuario normal se tecldea: <i>NombreEnrutador&gt;enable</i> Y se introduce el password en caso de estar configurado. Se obtiene el prompt <i>NombreEnrutador#</i>
Modo de configuración global.	Del modo de configuración de usuario privilegiado se tecldea: <i>NombreEnrutador#config terminal</i> Se obtiene el prompt: <i>NombreEnrutador(config)#</i>
Modo de configuración de interfaz.	Del modo de configuración global se tecldea: <i>NombreEnrutador#interfaze {nombre_y_número_interfaz}</i> Se obtiene el prompt: <i>NombreEnrutador(config-if)#</i>
Modo de configuración de enrutamiento.	Del modo de configuración global se tecldea el comando <i>NombreEnrutador(config)#router {protocolo de enrutamiento}</i> Donde el argumento es el protocolo de enrutamiento a configurar: Se obtiene el prompt: <i>NombreEnrutador(config-router)#</i>
Modo de configuración de sub-interfaz.	Solo se puede utilizar en una interfaz serial con encapsulamiento Frame Relay Se obtiene el prompt: <i>NombreEnrutador(config-subif)#</i>

Cada comando que se utilice debe de ser introducido en el modo de configuración correcto, para ello es necesario conocer el prompt desde el que se debe ejecutar el comando, si es que no se especifica explícitamente el modo desde el que se debe estar.

### 11.2.2 Configuración IP de un enrutador.

A continuación se detalla el procedimiento a realizar en un enrutador para configurar en él las direcciones IP de cada una de sus interfaces.

Este procedimiento se realiza en cada interfaz del enrutador que requiera trabajar con IP y se realiza en cada uno de los equipos de la red, por lo que es un procedimiento que se realizará frecuentemente.

Para configurar la dirección IP y su máscara en una interfaz lógica o física, se utiliza el siguiente comando en modo de configuración de interfaz:

```
NombreEnrutador(config-if)#ip address {dirección_ip} {network_mask}
```

La IP debe estar en el formato decimal con puntos al igual que la máscara de subred.

Para activar la interfaz y que empiece a operar se usa:

```
NombreEnrutador(config-if)#no shutdown
```

### 11.2.3 Configuración de encapsulamiento en interfaces seriales.

Hay varios tipos de encapsulamiento disponibles para ser usados en conexiones seriales. La elección de alguno por otro no es tan importante por que todos trabajan igual, lo que varía es el formato de la transmisión. Por lo que entre si son incompatibles, es decir un enrutador corriendo con Encapsulación PPP no tendrá comunicación con otro ejecutando HDLC.

En si el trabajar con varios tipos de encapsulamiento podrá ser incluido en las practicas del laboratorio.

A continuación se presenta los tipos de encapsulamiento más comunes.

#### 11.2.3.1 Encapsulación HDLC.

Este es el tipo de encapsulamiento serial por default en los equipos Cisco. Si todos los equipos conectados son de este fabricante se puede dejar este tipo de encapsulamiento y trabajarán sin problemas. Sin embargo si se trabaja con equipos de otros fabricantes que no tengan soporte para HDLC será necesario utilizar PPP u otro protocolo que soporten ambos equipos conectados.

El comando para reestablecer este tipo de encapsulación es el siguiente.

```
NombreEnrutador(config-if)#encapsulation hdlc
```

#### 11.2.3.2 Encapsulación PPP.

La Encapsulación PPP es la más común en casi cualquier tipo de equipo que realice comunicaciones seriales.

Este protocolo admite dos tipos de autenticación: CHAP y PAP.

El protocolo PPP con autenticación Challenge Handshake Authentication Protocol (CHAP) o Password Authentication Protocol (PAP) es frecuentemente usado para informar al sitio central acerca de cuáles enrutadores remotos están conectados a él.

Con esta información de autenticación, si el enrutador o el servidor de acceso recibe otro paquete para un destino al que ya esta conectado no realiza una llamada adicional.

Para usar autenticación CHAP o PAP, se debe tener corriendo encapsulación PPP en la interfaz.

CHAP y PAP están especificados en la RFC 1334. Estos protocolos están soportados en interfaces seriales sincronicas y asincronicas. Cuando se usa autenticación CHAP o PAP cada enrutador o servidor de acceso se identifica a si mismo por un nombre, este proceso de identificación previene el acceso no autorizado.

El control de acceso usando Challenge Handshake Authentication Protocol (CHAP) o Password Authentication Protocol (PAP) está disponible en todas las interfaces seriales que usan encapsulación PPP. La

característica de autenticación reduce el riesgo de violación de seguridad en el enrutador o servidor de acceso. Se puede configurar ya sea CHAP o PAP en la interfaz.

Cuando CHAP esta habilitado en una interfaz y un equipo remoto trata de conectarse a ella, el enrutador local envía un paquete CHAP al dispositivo remoto. El paquete CHAP pide o reta al equipo remoto a responder el reto que consiste de un ID, un numero aleatorio y el nombre del host local.

La respuesta al reto requiera consta de dos partes:

- Una versión encriptada del ID, un password secreto o "secret" y el numero aleatorio.
- Ya sea el nombre del host remoto o el nombre del usuario en el equipo remoto.

Cuando el enrutador local o servidor de acceso recibe la respuesta, verifica el secreto al realizar la misma operación de encriptación como se indicó en la respuesta y mira el nombre de usuario o host enviado. El password secreto debe ser idéntico en el dispositivo remoto y en el enrutador local. Al transmitir la respuesta el password o "secret" nunca es transmitido en texto plano, lo que previene que otros dispositivos de robarlo y ganar acceso ilegal al sistema. Sin la respuesta adecuada el dispositivo remoto no se puede conectar al enrutador local.

Las transacciones CHAP ocurren al mismo tiempo que el enlace es establecido. El enrutador local no requiere un password durante el resto de la llamada.

Cuando PAP esta habilitado el enrutador remoto que está tratando de conectarse al enrutador local es requerido a enviar una petición de autenticación. Si el nombre de usuario y el password en la petición son aceptados el IOS envía el acuse de recibo de la autenticación.

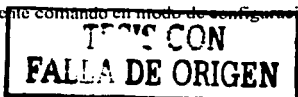
Después de que se ha habilitado CHAP o PAP, el enrutador local requiere autenticación de los dispositivos remotos.

Si el enrutador remoto no soporta el protocolo habilitado, ningún tráfico pasará por tal dispositivo.

Para usar la autenticación CHAP o PAP se requieren realizar las siguientes tareas:

Habilitar la encapsulación PPP en la interfaz con el siguiente comando en modo de configuración de interfaz.

*NombreEnrutador(config-if)#encapsulation ppp*



Habilitar CHAP o PAP en la interfaz.

Para CHAP, configurar la autenticación del nombre de host y el password o secreto para cada sistema remoto para el cual se requerirá autenticación.

Para definir el método de autenticación soportado y el orden en el cual será usado se usa el comando en modo de configuración de interfaz siguiente:

*NombreEnrutador(config-if)#ppp authentication {chap | chap pap | pap chap | pap} [if-needed] [list-name] [default] [callin]*

El argumento opcional {if-needed} puede ser usado solo con TACACS+. Los restantes argumentos se usan con Authentication, Authorization, and Accounting (AAA) si esta configurado en el enrutador.

### 11.2.3.3 Encapsulación Frame Relay.

Frame Relay es un protocolo de capa 2 ya descrito anteriormente. La conexión a una red Frame Relay es hecha con un loop local de la interfaz serial de un enrutador a la de un Switch Frame Relay de un proveedor de servicio.



La comunicación a través de una red Frame Relay es por medio de circuitos virtuales, los cuales están contruidos por un proveedor de servicio de la interfaz serial del enrutador a través de una colección de switches Frame Relay a otra interfaz serial de otro enrutador.

Los circuitos virtuales que están programados en la red de un proveedor para estar activos todo el tiempo son llamados circuitos virtuales permanentes o PVCs.

Muchos PVCs pueden ser contruidos en un solo loop local y son diseccionados con identificadores de conexión de enlace de datos o DLCI a nivel de capa 2.

Cada PVC tiene dos DLCI, uno en cada extremo, los cuales cambian de valor a través de todos los enlaces entre switches dentro de la nube Frame Relay

Cuando un enrutador quiere transmitir un paquete, debe de conocer el DLCI local del enrutador al que quiere enviar el paquete. Al hacerlo el Switch o switches intermedios saben que ese DLCI pertenece a tal circuito virtual y transmiten dicho paquete hasta llegar al equipo destino.

Si un enrutador tiene varios PVC en una misma interfaz, cada uno de ellos deberá tener su propio DLCI.

Hay dos maneras de configurar Frame Relay en un enrutador.

- Modelo Non Broadcast Multiple Access (NBMA.)

En el modelo NBMA la red Frame Relay es tratada como una red multi-acceso como una LAN, pero sin la facultad de broadcast, ya que no hay dirección de broadcast en Frame Relay. Todos los enrutadores conectados a una red NBMA comparten una dirección de red tal como una subred IP o un Cable Range de AppleTalk.

- Modelo de subinterfases.

En este modelo se tratan a cada una de los PVCs como una red lógica punto a punto separada, lo cual es hecho al crear una subinterfaz por cada PVC, lo cual requiere mas direcciones de red, dado que cada PVC tiene su propia dirección de red.

La configuración del NBMA consiste en instruir al IOS para realizar el encapsulamiento Frame Relay en la interfaz serial a la cual nuestro loop local de Frame Relay está conectado. Esto se hace con el comando de configuración de interfaz siguiente:

```
NombreEnrutador(config-if)#encapsulation frame-relay {ietf}
```

El argumento {ietf} es opcional y especifica usar la encapsulación definida por el IETF.

Después de esto es necesario configurar el enrutamiento en capas superiores.

Dado que una red NBMA es tratada como una red simple con múltiples hosts, todas las interfaces seriales conectadas a la red Frame Relay están en la misma subred IP, por lo que hay que configurarla interfaz con la dirección IP destinada para ello.

Cuando un paquete debe atravesar la red Frame Relay, el enrutador debe de tener una dirección de capa dos para ponerla en el encabezado de la trama, dicha dirección es el DLCI local del PVC que conduce al otro extremo, lo cual es hecho por InARP.

Si queremos poner mapeos manuales con el comando en modo de configuración de interfaz:

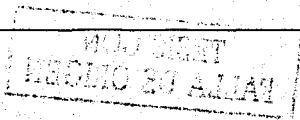
```
NombreEnrutador(config-if)#frame-relay map ip {ip_address} {número_DLCI} broadcast
```

Que nos permite definir estáticamente el DLCI local para alcanzar un host de red.

La configuración en el método de subinterfases es solo una interfaz lógica que está directamente asociada a una interfaz física.

Con la configuración de interfaz de Frame Relay podemos crear una subinterfaz para cada uno de los PVCs en una interfaz serial.

Hay dos tipos de subinterfases que pueden ser creadas por Frame Relay.



- Multipunto
- Puede manejar múltiples PVCs y su uso es similar al de la red NBMA
- Punto a punto.

Vuelve a cada PVC en una red punto a punto con su propio direccionamiento de red. Con este tipo se puede tener un control más grande sobre la red Frame Relay.

En interfaces que únicamente tienen un DLCI no es necesario hacer ninguna configuración adicional a la hecha con el modelo NBMA salvo usar una dirección IP dentro de una subred dedicada al enlace punto a punto.

En el caso de existir interfaces con más de un DLCI es necesario crear una subinterfaz por cada DLCI. Por cada subinterfaz hay una dirección IP perteneciente a la subred única asociada a la red punto a punto. Dado que la interfaz física normalmente no necesita direccionamiento, no es necesario asignarle una dirección IP

El comando en modo de configuración de interfaz (física) para crear subinterfaces (interfaces lógicas) es:  
*NombreEnrutador(config-if)#interface {subinterfaz} point-to-point*

Con este comando se crea una subinterfaz con el nombre de la original seguido por un punto y el número de la nueva subinterfaz.

El argumento point-to-point indica punto a punto pero también se permite el "multipoint"  
 Después el prompt cambia y se ingresa al modo de configuración de subinterfaz.

Enseguida se asigna un DLCI a dicha subinterfaz con el siguiente comando:

*NombreEnrutador(config-subif)#frame-relay interface-dlci dlci [ietf] cisco*

Donde:

{dlci} es el número de DLCI a usarse en la interfaz.

{ietf | cisco} es un argumento opcional para definir el tipo de encapsulación usada en la interfaz.

Para poder crear una subinterfaz lógica, es necesario haber habilitado previamente la Encapsulación Frame Relay en la interfaz física.

El proceso de asignación de direcciones IP a cada subinterfaz es el mismo de siempre. Pero si se desea se pueden utilizar otros protocolos de capa 3.

Como últimos comentarios se puede decir que el método más recomendado es el de subinterfaces, ya que en el modelo NBMA se tiene el problema de Split-horizon.

Para remover Frame Relay de una interfaz se usa el comando:

*NombreEnrutador(config-if)#no encapsulation frame-relay*

#### 11.2.4 Mapeo de direcciones de hosts y tareas comunes.

El nombre del enrutador por default es router (en inglés), pero para cambiarlo se utiliza el comando en modo de configuración global:

*NombreEnrutador(config)#hostname {Nuevo\_Nombre}*

Añadir una entrada para mapear un nombre de host a direcciones IP.

*NombreEnrutador(config)#ip host hostname {Número\_Puerto\_TCP} address {dirección\_IP}*

Donde:

{hostname} es el nombre del host a añadir a la tabla de host local.

{ Número\_Puerto\_TCP } es el número de Puerto TCP. Por default es 23 de Telnet.

Especificar el nombre de dominio que será añadido por el IOS a un nombre de host incompleto o no calificado.

*NombreEnrutador(config) #ip domain-name {nombre\_de\_dominio}*

Donde:

{nombre\_de\_dominio} es el nombre de dominio que se agregará.

Especificar la dirección o direcciones IP de servidores DNS

Máximo 6 DNS. La dirección por default es 255.255.255.255 (broadcast local)

*NombreEnrutador(config) #ip name-server {DNS1 DNS2 ... DNS6}*

Activar resolución de direcciones IP.

Por default esta activado, pero en caso de estar desactivado se activa con el comando siguiente:

*NombreEnrutador(config) #ip domain-lookup*

Verificación de la tabla local de hosts.

Con este comando se puede ver la tabla local de las direcciones de hosts conocidas.

*NombreEnrutador#show hosts*

### 11.2.5 Configuración del enrutamiento estático.

Una ruta estática es aquella que ha sido configurada manualmente en la tabla de enrutamiento. Tiene la ventaja de que no se necesitan protocolos de enrutamiento dinámicos, lo cual reduce la carga de CPU y memoria a los enrutadores. Es útil en redes pequeñas pero en redes grandes es muy difícil de mantener en perfecta operación.

Una ruta estática se agrega con el comando:

*NombreEnrutador(config)#ip route {network} {subnetmask} {ip\_address}*

Donde:

{network} es la dirección IP de la ruta agregada.

{subnetmask} es la máscara de subred de la red agregada

{ip\_address} es la dirección IP de la siguiente interfaz en el enrutador vecino.

Para remover se usa el comando inverso.

*NombreEnrutador(config)#no ip route {network} {subnetmask} {ip\_address}*

### 11.2.6 Configuración de enrutamiento por default.

Una ruta por default es aquella especificada a seguir por los datos si no hay información de enrutamiento específica para encontrar su destino.

El comando para especificar estáticamente la ruta por default es en el modo de configuración global:

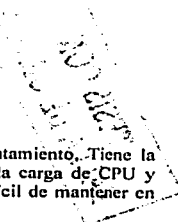
*NombreEnrutador(config)#ip default-network {ruta\_por\_default}*

Donde:

{ruta\_por\_default} es la dirección IP del host conectado directamente al que se enviarán los paquetes en caso de no poderse determinar su destino.

Este comando solo puede usarse si la red es conocida dentro de la tabla de enrutamiento local, por lo que casi no es usada.

En su lugar se puede usar el siguiente comando:



**NombreEnrutador(config)#ip route prefix mask sip-address [tipo-interfaz numero-interfaz [ip-address]] [distancia]**

Donde:

{prefix mask}. Prefijo y máscara de la ruta IP del destino.

{ip-address} es la dirección IP del siguiente salto que puede ser usado para alcanzar dicha red.

{tipo-interfaz, numero-interfaz} es el tipo y número de interfaz de red usada.

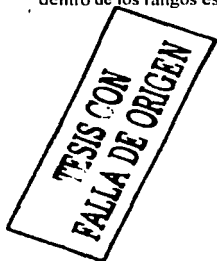
[distancia] es un argumento opcional para especificar la distancia administrativa.

### 11.2.7 Configuración de listas de acceso para filtrar servicios no permitidos.

El filtrado de paquetes se hace a través de listas de acceso en las interfaces de los enrutadores.

Al configurar listas de acceso se usan reglas para permitir o negar el paso de paquetes, cada lista de acceso se identifica con un número.

Todas las entradas en una lista de acceso deben tener el mismo número, dicho número puede ser elegido dentro de los rangos especificados en la siguiente tabla:



Protocolo	Rango
IP	1-99
IP extendido	100-199
Código de tipo Ethernet	200-299
DECNet	300-399
XNS	400-499
XNS extendido	500-599
Apple Talk	600-699
Dirección Ethernet	700-799
IPX	800-899
IPX extendido	900-999
IPX SAP	1000-1099

Tabla 11.1.2.7.1 Rangos de listas de acceso para diversos protocolos.

El enrutador procesa cada línea de cada lista de acceso en secuencia, contra cada paquete IP. Si una vez que alcanza el fin de la lista de acceso y no ha encontrado una coincidencia explícita para el paquete, este será descartado. lo que es conocido como un "deny any" implícito, por lo que es necesario que cada lista de acceso contenga al menos una orden que permita el paso de algún tipo de paquete.

Hay tres tipos básicos de listas de acceso IP.

- Estándar

Usa direccionamiento de la fuente para aplicar las reglas, lo que permite formas muy básicas de filtrado.

- Extendida.

Usa tanto las direcciones fuente como las direcciones destino para el filtrado, así como por tipo de protocolo. Por lo que permite un filtrado más granular.

- Dinámica.

Controla el flujo de paquetes en una base por usuario a través de un proceso de autenticación.

El enrutador usa una wildcard mask o máscara inversa para identificar un rango de direcciones para comparar junto con la dirección IP de una fuente o destino. Al igual que una máscara de red indica al enrutador cuáles bits de la dirección IP pertenecen a la dirección de red, la wildcard indica cuáles bits de la dirección IP necesita examinar para determinar la concordancia.

Un "1" en la wildcard mask significa "don't care" o sea que los bits correspondientes en la dirección IP no son considerados.

Hay dos palabras que pueden ser usadas para ahorrarnos el escribir mucho en las listas de acceso.

Any	La cuál puede usarse en lugar de 0.0.0.0 255.255.255.255 la cual significa cualquier combinación de bits en la dirección IP
Host	La cual puede ser usada en listas de acceso extendidas en vez de la máscara 0.0.0.0

En una lista de acceso estándar, omitir la máscara 0.0.0.0 es lo mismo que especificarla. Es decir, si se omite la wildcard mask, la dirección será considerada como una dirección de host.

Todas las listas de acceso estándar son definidas en el modo de configuración global. El comando y la sintaxis es la siguiente:

**NombreEnrutador(config)#access-list {número\_de\_lista\_de\_acceso} {deny | permit} {fuente [wildcard\_fuente]} any**

El número de la lista de acceso es un número dentro del rango específico que será en adelante el nombre de la lista.

{fuente} es la dirección fuente a la que aplicar la regla.

La wildcard\_fuente indica cuantos bits en el campo de la dirección son comparados

Las listas de acceso necesitan de un último paso para ser funcionales: especificar en que interfaz han de ser aplicadas.

Una cosa que debemos recordar es que si se aplica una lista a una interfaz antes de que se definan las entradas o si se niega una lista existente que ha sido aplicada, se tendrá una lista indefinida.

Se tiene dos opciones si queremos aplicar una lista de acceso como un filtro de paquetes:

Se puede aplicar una lista de acceso a una interfaz a manera de filtro de entrada o a manera de filtro de salida. Los filtros de salida son menos intensivos en el uso de procesador.

El comando para poner una interfaz en el grupo de interfaces que usan una lista de acceso para el filtrado de paquetes es en el modo de configuración de esa interfaz:

**NombreEnrutador(config-if)#ip access-group {número\_de\_lista\_de\_acceso} {out | in}**

Una misma lista de acceso puede ser usada en varias interfaces sin necesidad de definir una lista idéntica para cada interfaz.

El argumento "out" es el que se tiene por default y si se omite al escribirlo no importa. Con él se filtran los paquetes que salen del enrutador por esa interfaz.

Para crear un filtro de entrada se usa el argumento "in".

Si se requieren filtros de entrada y de salida de una interfaz se necesitan usar dos filtros, uno en cada dirección. Solo se puede aplicar una lista de acceso por protocolo, por interfaz y por dirección a la vez.

Una característica importante de las listas de acceso es el "deny any" implícito al final de todas que se agrega automáticamente por lo que toda lista debe de tener al menos un "permit" explícito.

Las listas de acceso extendidas permiten controlar el tráfico en una manera mas granular. Muchas de las reglas de las listas de acceso IP estándar son las mismas que para las extendidas, como:

- No se pueden añadir a mover líneas selectivamente de las lista, todo lo que se agrega va al final.
- Las listas de acceso necesitan ser aplicadas a interfaces para que trabajen.
- Al final de la lista hay por default un "deny any"

La sintaxis para crear una línea en una lista de acceso extendida es en el modo de configuración global:

**NombreEnrutador(config)#access-list {número\_de\_lista\_de\_acceso} {deny | permit} {protocolo} {fuente [wildcard\_fuente]} {destino [wildcard\_destino]}**

Por protocolo se especifica el tipo de protocolo a usar, como tcp, udp, icmp o ip.

Los demás argumentos indican la fuente y destinos específicos o una wildcard como "any"

---

La forma en que se aplican las listas de acceso a las interfaces es la misma que en listas de acceso estándar.

Cuando se esta planeando una lista de acceso, hay dos diferentes formas de hacerlo.

Si se sabe exactamente qué tráfico se quiere permitir, y se puede describir este tráfico en unas pocas líneas, se puede permitir ese tráfico y negar cualquier otro.

Si se puede describir el tráfico que se quiere evitar en unas pocas líneas, se puede negar el tráfico y permitir el resto con una línea al final "permit any"

### 11.2.8 Configuración NAT del enrutador.

Los comandos principales usados para configurar NAT son los siguientes:

- Para designar que el tráfico originado de o destinado a una interfaz esta sujeto a traducción de dirección de red (NAT) se usa el comando siguiente:

*ip nat {inside | outside} [log {translations syslog}]*

{inside} Indica que la interfaz está conectada a la red interna o la red que va a ser sujeta a la traducción.

{outside} Indica que la interfaz está conectada a la red externa

{log} habilita registro NAT.

{translations} Habilita el registro de traducciones NAT.

{syslog} Habilita syslog para el registro de traducciones NAT.

Para prevenir que la interfaz sea capaz de traducir se usa la forma no de este comando.

- Para habilitar traducción de la dirección de dirección destino interior se usa el comando en modo de configuración global siguiente:

*ip nat inside destination list {access-list-number | name} pool name*

list {access-list-number | name} Número o nombre de una lista de acceso estándar. Los paquetes con la dirección destino que pasan la lista de acceso son traducidas usando direcciones globales del pool mencionado.

{pool name} Nombre del pool del cual direcciones globales IP son usadas durante la traducción dinámica.

Este comando tienes dos formas; la traducción dinámica y la traducción estática, la forma con la lista de acceso establece una traducción dinámica.

Los paquetes con direcciones que concuerdan con la lista de acceso estándar son traducidos usando direcciones globales obtenidas del pool nombrado con el comando "ip nat pool" que se explica más adelante. Para remover la asociación dinámica al pool se usa la forma no de este comando.

*no ip nat inside destination list {access-list-number | name} pool name*

- Para habilitar traducción de la dirección de dirección fuente interior se usa el comando de configuración global siguiente:

*ip nat inside source {list { access-list-number | name} pool name [overload] | static local-ip global-ip}*

{list access-list-number | name} Número o nombre de lista de acceso estándar. Los paquetes con direcciones fuente que pasen por esta lista son traducidos dinámicamente usando direcciones globales del pool especificado.

{pool name} Es el nombre del pool del cual las direcciones IP son asignadas dinámicamente.

{overload} (Opcional) Habilita al enrutador para usar una dirección local para muchas direcciones locales.

**{static local-ip}** Establece una traducción única, este argumento establece la dirección IP local asignada a un host de la red interior. La dirección puede ser elegida ya sea aleatoriamente, o de la RFC 1918.

**{global-ip}** Establece la traducción estática única, este argumento establece la dirección IP globalmente única de un host interior como si fuera del mundo exterior.

Por default no hay traducción NAT de direcciones fuente interior.

Este comando tiene dos formas; la traducción dinámica y la traducción estática.

La forma con una lista de acceso estándar establece una traducción dinámica. La sintaxis con la palabra "static" establece una traducción única.

Para remover la traducción estática o mover la asociación dinámica a un pool se usa la forma "no" de este comando.

- Para habilitar traducción NAT de la dirección fuente exterior se usa en el modo de configuración global el comando siguiente. Para removerlo se usa la forma no del mismo.

*ip nat outside source {list {access-list-number | name} pool name | static global-ip local-ip}*

**{list access-list-number | name}** Número o nombre de lista de acceso estándar. Los paquetes con direcciones fuente que pasen por esta lista son traducidos dinámicamente usando direcciones globales del pool especificado.

**{pool name}** Es el nombre del pool del cual las direcciones IP son asignadas dinámicamente.

**{static global-ip}** Establece una traducción única, este argumento establece la dirección IP globalmente única asignada a un host en la red exterior por su dueño

**{local-ip}** Establece una traducción única, este argumento establece la dirección IP local de un host exterior como si apareciera en el mundo interior. La dirección fue asignada del espacio enrutable de direcciones según la RFC 1918.

Se pueden usar direcciones IP que no son legalmente u oficialmente asignadas. Ya que tal vez estén asignadas a alguien más. El caso de que una dirección IP es usada legal e ilegalmente se llama "overlapping". Se puede usar NAT para traducir direcciones interiores que se enciman con direcciones exteriores.

Este comando tiene dos formas; la traducción dinámica y la traducción estática.

La forma con una lista de acceso estándar establece una traducción dinámica. La sintaxis con la palabra "static" establece una traducción sola.

- Para definir un pool de direcciones para NAT se usa el comando siguiente en modo de configuración global.

*ip nat pool name start-ip end-ip {netmask máscara | prefix-length prefix-length} {type rotary}*

Este comando define un pool de direcciones usando una dirección de inicio, una dirección de final y una máscara o prefijo.

El pool puede definir ya sea un pool interior global o un pool exterior local o un "rotary pool"

**{name}** Nombre del pool.

**{start-ip}** Dirección IP de inicio que define el rango de direcciones en el pool de direcciones.

**{end-ip}** Dirección IP final que define el rango de direcciones en el pool de direcciones.

**{netmask máscara | prefix-length prefix }** Indica ya sea la máscara de red o el prefijo asociado que indica cuáles bits de dirección pertenecen a los campos de red y subred y cuáles bits a l campo de host. Especifica la máscara de red a la cual pertenece el pool de direcciones.

**{type rotary}** (Opcional) Indica que el rango en el pool de direcciones identifica hosts interiores reales entre los cuales puede ocurrir distribución de carga TCP.

- Para cambiar la cantidad de tiempo después de expiran las traducciones NAT, se usa el comando en modo de configuración global siguiente, para deshabilitarlo se usa la forma no de este comando.

La sintaxis es la siguiente:

*ip nat translation [max-entries number] [timeout | udp-timeout | dns-timeout | tcp-timeout | finrst-timeout | icmp-timeout | pptp-timeout | syn-timeout | port-timeout] seconds | never*

Donde:

{max-entries number} (Opcional) Especifica el número máximo de entradas NAT (1-2147483647).

{timeout} Especifica que el valor de timeout aplica a traducciones dinámicas excepto para traducciones por overloading El {default es 86400 segundos (24 horas)}.

{udp-timeout} Especifica que el valor del timeout aplica al puerto UDP. El Default es 300 segundos (5 minutos).

{dns-timeout} Especifica que el valor del timeout aplica a conexiones a DNS. El default es 60 segundos.

{tcp-timeout} Especifica que el valor del timeout aplica al puerto TCP. El default es 86400 segundos (24 horas).

{finrst-timeout} Especifica que el valor del timeout aplica a paquetes TCP finish y reset, los cuales terminan la conexión. El default es 60 segundos.

{icmp-timeout} Especifica el valor del timeout para flujo ICMP. El default es 60 segundos.

{pptp-timeout} Especifica el valor del timeout para flujo Point-to-Point Tunneling Protocol (PPTP) El default es 86400 segundos (24 horas).

{syn-timeout} Especifica el valor del timeout para flujo TCP inmediatamente después de un SYN. El default es 60 segundos.

{port-timeout} Especifica que el valor del timeout aplica al puerto TCP/UDP.

{seconds} Numero de segundos después de los cuales la traducción del puerto especificado expira. Los valores por default están esta listados arriba.

{never} Especifica que no haya tiempo de expiración en la traducción de puerto.

Los valores por default son los siguientes:

<ul style="list-style-type: none"><li>• El timeout default es 86,400 segundos (24 horas)</li><li>• udp-timeout es 300 segundos (5 minutos)</li><li>• dns-timeout es 60 segundos (1 minuto)</li><li>• tcp-timeout es 86400 segundos (24 horas)</li><li>• finrst-timeout es 60 segundos (1 minuto)</li></ul>	<ul style="list-style-type: none"><li>• icmp-timeout es 60 segundos (1 minuto)</li><li>• pptp-timeout es 86400 segundos (24 horas)</li><li>• syn-timeout es 60 segundos (1 minuto)</li><li>• port-timeout es 0 (nunca)</li></ul>
--	--

Cuando la traducción de puerto está configurada, hay un control más fino sobre los tiempos de expiración de la traducción dado que cada entrada contiene más contexto acerca del tráfico que está usando.

Una vez repasados los comandos que se utilizan para configurar NAT es necesario saber los pasos de diseño que se necesitan seguir para implementarlo, los cuales son:

- a) Se deben definir las interfaces interiores y exteriores NAT, para ello se debe saber si hay interfaces múltiples que se conectan a Internet.  
En nuestro caso solo contamos con una interfaz interior y una interfaz exterior, la interfaz exterior es una Ethernet que nos conectará al segmento de red donde se encuentra el quipo de salida a Internet y los servidores.
- b) Se debe definir lo que se está intentando lograr con NAT. En nuestro caso se intenta permitir a usuarios internos el acceso al Internet, y permitir a usuarios externos el tener acceso a los dispositivos internos, tales como el Access Server y los enrutadores.
- c) Verificar la operación NAT.



Como se describió en los comandos de configuración, NAT tiene varias variantes, que son:

- NAT Estático.
- La tabla de traducción se configura manualmente en el enrutador sin necesidad de que haya tráfico.
- NAT Dinámico.
- La tabla de traducción se va llenando conforme el tráfico que pasa por el enrutador necesita ser traducido.
- Overloading.

En esta configuración, solo se utiliza una dirección IP válida para mapear varias direcciones IP inválidas. Para nuestros fines de configuración de NAT, al laboratorio lo podemos representar con el siguiente esquema de diseño:

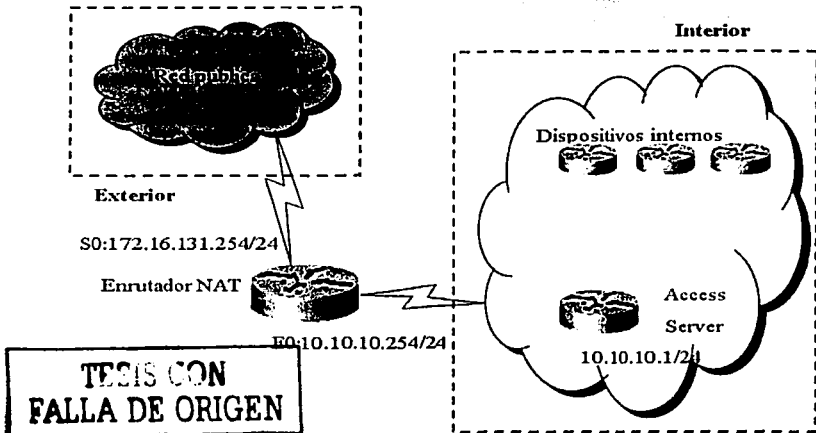


Figura 11.1.2.8.1 Esquema de implementación de NAT.

La red exterior o pública son todos aquellos dispositivos que utilizan direcciones IP válidas o que pertenecen a otras redes. La red interior son nuestros dispositivos sujetos a traducción NAT.

En nuestro caso utilizaremos tanto NAT estático como NAT dinámico. Por otra parte, aunque se espera contar con un bloque pequeño de direcciones IP disponibles, mostraremos la manera de configurar NAT con y sin overloading.

#### Permitir que los usuarios internos tengan acceso al Internet

Deseamos que NAT permita que ciertos dispositivos en el interior originen la comunicación con los dispositivos en el exterior traduciendo su dirección inválida a una dirección válida o pool de direcciones. Como ejemplo se ha definido el pool como la gama de las direcciones 172.16.10.1 a 172.16.10.63, es decir un bloque de 63 direcciones.

El primer paso es instruir al enrutador que una interfaz en particular será una interfaz NAT interna o externa. Esto se puede hacer cuando se está configurando la dirección IP, en modo de configuración de interfaz.

La configuración del enrutador en el respectivo a NAT quedaría como sigue:

---

```
interface ethernet 0
ip address 10.10.10.254 255.255.255.0
ip nat inside
```

```
interface serial 0
ip address 172.16.131.254 255.255.255.0
ip nat outside
```

#### **Configuración para usar NAT dinámico sin overloading.**

Se define un pool de direcciones llamado llamado no-overload con un rango de direcciones de 172.16.10.1 a 172.16.10.63 y luego se indica que cada paquete recibido en la interfaz interior, permitido por la lista de acceso 7 tendrá la dirección fuente traducida a una dirección fuera del pool NAT "no-overload". La lista de acceso 7 permite el paso de paquetes con una dirección fuente dentro del rango 10.10.10.0 a 10.10.10.31

```
ip nat pool no-overload 172.16.10.1 172.16.10.63 prefix 24
ip nat inside source list 7 pool no-overload
access-list 7 permit 10.10.10.0 0.0.0.31
```

En la configuración anterior solamente las primeras 32 direcciones de la subred 10.10.10.0 se permiten por la lista de acceso 7. Por lo tanto, solamente se traducen estas direcciones de la fuente. Aunque puede haber otros dispositivos con otras direcciones en la red interior, pero éstos no serán traducidos.

#### **Configuración par usar NAT dinámico usando overloading.**

Para esto se traducen cada una de las direcciones de los dispositivos interiores a una dirección válida única. Solamente debemos cambiar la definición de NAT y del pool anteriores.

Se define un pool NAT llamado pool\_sobrecargado con un rango de una sola dirección IP (172.16.10.1/24). Y se indica que cualquier paquete recibido en la interfaz interior que esté permitido por la lista de acceso 7 tendrá la dirección fuente trasladada a una dirección fuera del pool NAT llamado pool\_sobrecargado, las traducciones serán sobrecargadas lo cual permitirá múltiples dispositivos interiores para ser trasladados a la misma dirección IP válida

En esta configuración, el pool pool\_sobrecargado tiene solamente una gama de una dirección.

```
ip nat pool pool_sobrecargado 172.16.10.1 172.16.10.1 prefix 24
ip nat inside source list 7 pool pool_sobrecargado overload
```

Otra variación del método de overloading en el cual se configura NAT para sobrecargar la dirección que se asigna a la interfaz serial 0 es:

```
ip nat inside source list 7 interface serial 0 overload
```

Cuando este tipo de overloading se configura, el enrutador mantiene bastante información de protocolos de alto nivel (por ejemplo, los números de acceso del TCP o del UDP) para traducir la dirección global de nuevo a la dirección local correcta.

Para permitir a los dispositivos internos intercambiar información por los dispositivos en el Internet, como será el caso del Access Server para acceder a los equipos, es necesario utilizar NAT estático, ya que se deberá poder tener acceso a él, y será el único equipo con el que se podrá tener contacto desde el exterior.

Los dispositivos en el exterior deben poder originar la comunicación solamente con el Access Server en el interior.

Con NAT dinámico, las traducciones no existen en la tabla NAT de traducción hasta que el enrutador recibe el tráfico que requiere la traducción. Dinámicamente las traducciones tienen un período del descanso después del cual se purgan de la tabla de traducción NAT.

Con NAT estático, las traducciones existen en la tabla NAT de la traducción tan pronto como se configuran el o los comandos NAT estáticos, y sigue estando en la tabla de traducción hasta que se suprime NAT estático. Para configurar esto se utiliza el comando:

```
ip nat inside source static 10.10.10.1 172.16.131.1
```

Esta entrada traduce la dirección global del interior de nuevo a la dirección local del interior, que significa que los dispositivos en la nube exterior pueden enviar los paquetes a la dirección global 172.16.131.1 y alcanza el dispositivo en la nube interior, que tiene la dirección local 10.10.10.1.

### Verificar La Operación NAT

Una vez que se ha configurado NAT, se debe verificar que esté funcionando según lo esperado. Se puede hacer esto usando un analizador de red o con los comandos "show" o "debug"..

## 11.3 Conexión física entre dispositivos.

### 11.3.1 Conexión Ethernet en un enrutador.

La conexión Ethernet es simple de configurar, pero hay algunos puntos en los que hay que poner atención al momento de hacer la conexión.

En el pasado los enrutadores Cisco tenían una interfaz AUI (Attachment Unit Interface) para Ethernet, que es útil para 10base5, pero en caso de tener 10baseT o 10base2 se requiere de un "transceiver" o transductor conectado a la interfaz AUI para convertir la señal.

Los equipos Cisco más recientes, proveen una interfaz de medio dual para Ethernet; una con el receptáculo AUI y otra con el receptáculo RJ45.

Solo se puede usar una interfaz, por default es la AUI. Si se quiere usar la interfaz se requiere especificarlo con el comando en modo de configuración de la interfaz siguiente:

```
NombreEnrutador(config-if)#media-type 10baseT
```

### 11.3.2 Conexión "back-to-back" entre enrutadores.

Esta configuración se realiza cuando se conectan dos enrutadores a través de un cable serial V.35 directamente entre sus puertos seriales.

La siguiente figura ilustra el esquema de una conexión "back-to-back".



Figura 11.3.2.1 Conexión Back-to-back entre dos enrutadores.

El cable serial tiene dos extremos, uno de los cuáles trabaja como DTE y el otro como DCE, el enrutador que está conectado al extremo DCE debe ser configurado para generar el reloj de transmisión.

Si no sabemos como determinar cual es el enrutador con la punta que funciona como DCE se puede conectar el cable y usar el comando:

---

### *NombreEnrutador>show controller cbus*

Observando las líneas de salida del comando que corresponden a la interfaz serial de interés, podemos determinar cual es el extremo DCE.

A continuación se reproduce la configuración necesaria para poder conectar correctamente dos enrutadores en "back-to-back", considerando que el enrutador A es el que genera el reloj.

El enrutador A tiene conectado al puerto serial 0 la punta DCE, y el enrutador B la punta DTE al puerto serial 1.

A partir del modo de configuración global:

```
EnrutadorA(config)#interface serial 0
EnrutadorA(config-if)#clock rate {tasa_transmisión}
```

Donde:

{tasa\_transmisión} es la velocidad en bps.

Las consideraciones mencionadas se aplican por igual si entre los equipos se conecta un fraccionador en un enlace serial remoto, solo que habrá que configurar también el fraccionador con los canales adecuados y sincronizar los relojes de transmisión.

Adicionalmente se puede modificar el tipo de encapsulación por default que se realizara en el enlace. Por default es HDLC en equipos Cisco, pero se puede ocupar PPP u otro.

### **11.3.3 Configuración de un Switch o HUB Cisco.**

Después de instalar físicamente el dispositivo y alimentarlo correctamente se enciende el Switch, una vez encendido el equipo y que ha pasado el POST (El POST ha terminado cuando se prenden los LEDs en verde y luego se apagan), se conectan los cables. El POST es un programa de verificación de hardware que se ejecuta cada que se prende o reinicia el equipo.

Se debe usar cable uno a uno (straight-through) en los puertos que no están marcados con una X.

Se debe usar cable cruzado (crossover) en los puertos marcados con una X.

Se puede usar cable categoría 5 si al ancho de banda no pasa de 100 Mbps, excepto para 100Base FX y similares que requieren fibra óptica.

Se conecta después un cable entre el puerto de consola del Switch y el puerto de consola de una terminal vt100 o de un equipo corriendo software de emulación de terminal.

Se utilizan los menús que despliega el IOS del dispositivo para configurar la dirección IP y la máscara de subred asignados al equipo, el Default Gateway, los servidores DNS si es el caso y el método de conmutación en el caso de Switches.

Cada configuración surte efecto inmediatamente después de que se ejecuta el comando correspondiente, sin embargo en equipos más viejos es necesario reiniciar el equipo para que las configuraciones surtan efecto.

## **11.4 Configuración de protocolos de enrutamiento.**

### **11.4.1 Configuración del protocolo de enrutamiento RIP.**

Para configurar el protocolo de enrutamiento RIP es necesario entrar desde el modo de configuración global al modo de configuración de enrutamiento de este protocolo con el comando:

```
NombreEnrutador(config)#router rip
```

El comando para activar RIP en las interfaces que deseemos es:

---

**NombreEnrutador(config-router)#network {Máscara}**

Donde:

{Máscara} es una máscara de dirección IP que contiene las direcciones IP de las interfaces que deseamos que corran RIP.

Estos son los únicos comandos necesarios para poder ejecutar RIP en el enrutador, sin embargo, los comandos que se utilizan para cambiar y optimizar el funcionamiento de RIP son los siguientes:

Para cambiar entre las dos versiones de RIP: RIPv1 y RIPv2.

**NombreEnrutador(config-router)#versión {1 | 2}**

{1 | 2} Representa la versión que se quiere utilizar. Por default es 1.

Para especificar el tipo de versión usada en las actualizaciones tanto recibidas como enviadas, en interfaces específicas se usa:

**NombreEnrutador(config-if)#ip rip {send | receive} version {1 | 2}**

{send | receive} especifica la acción afectada en esa interfaz para recibir o enviar

{1 | 2} Especifica la versión a usar.

Cambio de distancia administrativa

**NombreEnrutador(config-router)#distance {Distancia}**

{Distancia} distancia administrativa a usar por RIP. Por default es 120.

Volver una interfaz pasiva.

**NombreEnrutador(config-router)#passive-interface {Interfaz}**

{Interfaz} especifica la interfaz para que se comporte como pasiva.

Para cambiar los timers que afectan el proceso de convergencia de RIP se utiliza el comando:

**NombreEnrutador(config-router)#timers basic {update | invalid | holddown | flush} {tiempo\_en\_segundos}**

{update | invalid | holddown | flush} especifica el timer que se quiere modificar

{tiempo\_en\_segundos} especifica el tiempo en segundos a usar en el timer especificado.

Los comandos para configurar más a fondo RIPv2 son los siguientes:

Para deshabilitar la autosumarización que por default realiza RIPv2.

**NombreEnrutador(config-router)#no auto-summary**

Para usar autenticación se usa en el modo de configuración de interfaz:

**NombreEnrutador(config-if)#ip rip authentication key-chain {Cadena}**

{Cadena} es el grupo de claves que son válidas.

Para usar autenticación en texto plano o en le formato MD5 se usa:

**NombreEnrutador(config-if)#ip rip authentication mode {text | MD5}**

---

{text | MD5} especifica el modo a usar.

#### 11.4.2 Configuración del protocolo de enrutamiento IGRP.

Para configurar el protocolo de enrutamiento IGRP es necesario entrar desde el modo de configuración global al modo de configuración de enrutamiento de este protocolo con el comando:

***NombreEnrutador(config)#router igrp {sistema\_autónomo}***

Donde:

{sistema\_autónomo} es un número que identifica a un sistema autónomo.

El comando para activar IGRP en las interfaces que deseamos es:

***NombreEnrutador(config-router)#network {Máscara}***

Donde:

{Máscara} es una máscara de dirección IP que contiene las direcciones IP de las interfaces que deseamos que corran IGRP.

Estos son los únicos comandos necesarios para poder ejecutar IGRP en el enrutador, los comandos que se utilizan para cambiar y optimizar el funcionamiento de IGRP son los mismos que en RIP además de los siguientes específicos para IGRP.

#### Aplicar Offsets a las métricas de enrutamiento.

Una lista de offset es el mecanismo para incrementar las métricas de entrada y salida a rutas aprendidas vía IGRP. Esto es hecho al proveer un mecanismo local para incrementar el valor de las métricas de enrutamiento.

Opcionalmente se puede limitar la lista de offset ya sea con una lista de acceso o una interfaz. Para incrementar el valor de métricas de enrutamiento se usa el comando siguiente en modo de configuración de enrutamiento.

***NombreEnrutador(config-router)#offset-list [access-list-number | name] {in | out} offset {type number}***

#### Deshabilitar Holddown.

Cuando el IOS aprende que una red está a una distancia más grande de lo que previamente se sabía, o ve que la ruta esta caída, dicha ruta es colocada en Holddown. Durante ese periodo la ruta es anunciada, pero los anuncios entrantes acerca de tal red de cualquier otro enrutador diferente que el original del que se aprendió la ruta son ignorados. Este mecanismo es frecuentemente usado para ayudar a prevenir loops de enrutamiento en la red. Pero tiene el efecto de incrementar el tiempo de convergencia de la topología de red.

Para deshabilitar holddown con IGRP se usa el comando siguiente en el modo de configuración de enrutamiento:

***NombreEnrutador(config-router)#no metric holddown***

#### Habilitar o deshabilitar Split Horizon.

Normalmente los enrutadores que están conectados a redes IP broadcast y que usan protocolos de enrutamiento de vector distancia, emplean el mecanismo de Split Horizon para reducir la posibilidad de loops de enrutamiento. En el Split Horizon se bloquea el anuncio de información acerca de rutas por la interfaz en que fue aprendida. Este comportamiento usualmente optimiza la comunicación entre enrutadores múltiples, particularmente cuando los enlaces están rotos.

De cualquier manera en redes no broadcast como Frame Relay, la situación que se puede crear por este comportamiento no es el ideal. Por tal razón es posible desear deshabilitar Split Horizon.

---

Para habilitar o deshabilitar Split Horizon se utiliza el comando en modo de configuración de interfaz siguiente:

*NombreEnrutador(config-if)#ip split-horizon*

Este comando aplica también para RIP.

Split Horizon esta deshabilitado por default en la encapsulación Frame Relay. Pero no en X.25 ni en otros tipos de encapsulación, en los que Split Horizon está habilitado por default.

### 11.4.3 Configuración del protocolo de enrutamiento EIGRP.

El proceso de configuración del protocolo de enrutamiento EIGRP es prácticamente igual al de IGRP, ya que es una versión mejorada en su desempeño más que en su funcionamiento.

EIGRP ofrece las siguientes características:

- Convergencia más rápida. El algoritmo dual permite enrutar información mas rápido que otros protocolos.
- Actualizaciones parciales. EIGRP envía actualizaciones incrementales cuando el estado del destino cambia, en lugar de enviar el contenido completo de la tabla de enrutamiento. Esta característica minimiza el ancho de banda requerido para los paquetes EIGRP.
- Menor uso de memoria y CPU que IGRP. Esto ocurre dado que los paquetes de actualizaciones no tienen que ser procesados cada que son recibidos.
- Mecanismo de descubrimiento de vecinos. Es un mecanismo simple usado para conocer enrutadores vecinos.
- Máscaras de subred de longitud variable.
- Sumarización de rutas arbitraria.
- Escalamiento a grandes redes.

#### Habilitar EIGRP

Para crear un proceso de enrutamiento EIGRP se usan los siguientes comandos en el modo de configuración global y de enrutamiento.

*NombreEnrutador(config)#router eigrp autonomous-system*

*NombreEnrutador(config-router)#network network-number*

#### Transición de IGRP a EIGRP

Si se tiene enrutadores configurados con IGRP y se quiere hacer la migración a EIGRP, se deben designar enrutadores de transición que tengan tanto IGRP como EIGRP configurado. Se debe de tener el mismo número de sistema autónomo para redistribuir las rutas automáticamente.

#### Deshabilitar sumarización de rutas.

Se puede configurar EIGRP para realizar sumarización automática de rutas de subredes a redes de mayor nivel.

Para deshabilitar sumarización automática se usa el siguiente comando en modo de configuración de enrutamiento.

*NombreEnrutador(config-router)# no auto-summary*

La sumarización de rutas trabaja en conjunción con el comando de configuración de interfaz siguiente:

*NombreEnrutador(config-if)#ip summary-address eigrp numero-sistema-autonomo direccion mask*

---

Donde:

numero-sistema-autonomo Es el número de sistema autónomo EIGRP.  
(direccion) es la dirección IP summarizada a aplicar a la interfaz.  
{mask} es la máscara de subred.

En el cual se puede realizar summarización adicional. Si la summarización esta trabajando, usualmente no hay necesidad de configurar niveles de red usando el comando anterior.

#### 11.4.4 Configuración del protocolo de enrutamiento OSPF.

Los detalles técnicos relevantes de OSPF fueron dados en los primeros capítulos

OSPF típicamente requiere coordinación entre muchos enrutadores internos, enrutadores de borde de área y enrutadores de límite de sistema autónomo.

Como mínimo, los enrutadores basados en OSPF o los servidores de acceso pueden ser configurados con todos los valores por default de los parámetros de OSPF, sin autenticación e interfaces asignadas a áreas. Si se intenta personalizar el entorno, se debe asegurar la configuración coordinada de todos los enrutadores.

Para poner en marcha OSPF en un enrutador se requiere habilitar dicho protocolo de enrutamiento tal como se ha hecho con otros protocolos. Para ello se crea el proceso de enrutamiento, se especifica el rango de direcciones IP a ser asociadas al proceso de enrutamiento y se asigna el ID de área para ser asociado con el rango de direcciones IP.

Para ello se ocupan los siguientes comandos empezando en modo de configuración global.

*NombreEnrutador(config)#router ospf process-id*

*NombreEnrutador(config-router)#network address wildcard-mask area {area-id}*

Donde:

{area-id} es el área a la que se integrara el enrutador en la red.

Las tareas siguientes son opcionales pero pueden ser requeridas dependiendo del tipo de implementación que se tenga en mente.

Nuestra implementación de OSPF nos permite alterar ciertos parámetros específicos OSPF. No es necesario cambiar todos los parámetros, pero se debe ser consistente y compatible en todos los enrutadores de la red.

Esos parámetros son controlados por los comandos siguientes:

**Especificar el costo de enviar un paquete en una interfaz OSPF.**

*NombreEnrutador(config-router)#ip ospf cost {costo}*

**Especificar el número de segundos entre retransmisiones de anuncios de rutas por estado de enlace**

*NombreEnrutador(config-router)#ip ospf retransmit-interval seconds*

**Establecer el número estimado de segundos que toma transmitir una actualización de estado de enlace en una interfaz OSPF.**

*NombreEnrutador(config-router)#ip ospf transmit-delay {seconds}*

**Establecer la prioridad para ayudar a determinar el "enrutador designado" para una red OSPF.**

*NombreEnrutador(config-router)#ip ospf priority {number}*

**Establecer la cantidad de tiempo entre paquetes Hello que el IOS envía en una interfaz OSPF**



---

*NombreEnrutador(config-router)#ip ospf hello-interval {seconds}*

Establecer el número de segundos antes de que un paquete Hello del enrutador no debe ser enviado antes de que sus vecinos declaren el enrutador OSPF caído.

*NombreEnrutador(config-router)#ip ospf dead-interval {segundos}*

Asignar un password para ser usado por enrutadores OSPF vecinos en un segmento de red que está usando autenticación de password simple.

*NombreEnrutador(config-router)#ip ospf authentication-key {clave}*

**Habilitar autenticación OSPF MD5**

*NombreEnrutador(config-router)#ip ospf message-digest-key keyid md5 key*

Especificar el tipo de autenticación para una interfaz.

*NombreEnrutador(config-router)#ip ospf authentication [message-digest | null]*

El software OSPF permite configurar varios parámetros de área OSPF. Estos parámetros de área incluyen autenticación definición de áreas Stub y asignación de costos específicos a la ruta sumariada default.

La autenticación permite protección basada en password contra acceso no autorizado en un área.

Las áreas Stub son áreas en las cuales la información de redes externas no es enviada. En lugar de eso hay una ruta externa por default generado por el enrutador de borde de área usada para destinos fuera del sistema autónomo.

Para tomar ventaja del soporte de área Stub se debe usar enrutamiento por default. Para reducir el número de anuncios de estado de enlace hacia el área Stub, se puede configurar el parámetro no-summary en el enrutador de borde de Área ABR.

Los comandos disponibles son los siguientes:

**Habilitar la autenticación en un área OSPF.**

*NombreEnrutador(config-router)#area {area-id} authentication*

**Habilita la autenticación MD5 en un área OSPF**

*NombreEnrutador(config-router)#area {area-id} authentication message-digest*

**Define un área para ser un área Stub**

*NombreEnrutador(config-router)#area {area-id} stub [no-summary]*

**Asigna un costo específico a la ruta por default del área Stub.**

*NombreEnrutador(config-router)#area {area-id} default-cost {cost}*

Con los comandos presentados se puede hacer una configuración básica e intermedia en una red basada en OSPF como protocolo de enrutamiento.

#### **11.4.5 Verificación del funcionamiento y operación de los protocolos de enrutamiento.**

---

Un enrutador puede estar ejecutando varios protocolos de enrutamiento. Para verificar el funcionamiento de ellos se puede usar el comando:

**NombreEnrutador>show ip protocols**

Y muestra información general de los protocolos de enrutamiento de IP que están ejecutándose en el IOS. Así como información específica de cada protocolo.

Otro comando útil para verificar el funcionamiento de uno o varios protocolos de enrutamiento es:

**NombreEnrutador>show ip route**

Este comando muestra la tabla de enrutamiento completa para IP; si se usa como argumento una red IP, solo se muestra la información de rutas de esa red.

Se muestran las rutas así como información de las subredes e interfaces asociadas, así como el protocolo del cual se aprendió dicha ruta.

Hay comandos específicos para cada uno de los diferentes protocolos de enrutamiento dependiendo de sus características propias, sin embargo no serán mencionados ya que con los mostrados, basta para hacer una implementación y una evaluación general del desempeño del protocolo.

Si se quiere hacer una revisión mas profunda del protocolo se deberán revisar los manuales de operación y configuración del mismo.

### **11.5 Resumen.**

En este capítulo se presentaron las diversas configuraciones y conexiones que son denominadas tipo, debido a que son procedimientos comunes en la implementación del laboratorio y que se repiten continuamente, por lo que no es necesario repetir las una y otra vez al momento de realizar tareas mas complejas. De esta manera se resumen a manera de que puedan servir de referencia al momento de implementar el laboratorio.

Sin embargo de ninguna manera son todos los procedimientos que pueden ser usados en la configuración del laboratorio, ni sustituto de los manuales y guías de instalación creados por el fabricante, ya que si es necesario obtener mas información respecto a algún protocolo, tecnología o comando específico, se deberá consultar dicha documentación.

## Capítulo 12.

### 12 Conexión a las consolas de equipos.

#### 12.1 Introducción.

La conexión de los equipos y de las consolas es un aspecto que debe definirse con exactitud, ya que es un elemento imprescindible en el diseño del laboratorio a fin de que éste pueda ser operacional.

La conexión y configuración de los equipos puede hacerse de dos maneras, con una conexión local o con una conexión remota. Para la conexión local se está físicamente cerca del equipo, con la ventaja de poder realizar maniobras de cambio en el cableado, que ocasionalmente puede ser un problema que solo puede solucionarse en sitio.

Para la conexión remota no se tiene la posibilidad de realizar cambios físicos en el equipo, además de que para poder trabajar en una sesión en forma remota, el equipo ya debe de estar configurado y trabajando en la red para poder acceder al mismo.

En este capítulo se definen los aspectos técnicos generales de las alternativas que se tiene para poder hacer la conexión a los enrutadores tanto en forma local como en forma remota. Para ello se necesita saber cuáles son los medios físicos como los medios lógicos usados para poder realizar dicha conexión.

#### 12.2 Líneas de terminal.

Las líneas de terminal son dispositivos físicos o lógicos del enrutador que nos permiten tener acceso a la interfaz de línea de comandos del IOS que está corriendo en el enrutador.

En un enrutador hay cuatro tipos de líneas de terminal.

- Puerto de consola (CTY o CON.)

Todos los enrutadores tienen un puerto de consola en la parte trasera del enrutador, dicho puerto proporciona una conexión serial asíncrona (EIA/TIA-232 o también conocida como RS-232), que nos permite comunicarnos con el enrutador.

El tipo de conexión física al puerto de consola depende del modelo de enrutador. Algunos usan un conector hembra DB25 y otros un conector RJ45. Como regla general los enrutadores de modelos menores tienen un conector de consola RJ45.

Nosotros vamos a trabajar con enrutadores Cisco de varios modelos, por lo que debemos familiarizarnos con algunas de sus características.

En la tabla siguiente se puede ver una lista del tipo de conector para el puerto de consola en diferentes series de enrutadores Cisco.

Cisco Series.	Conector de consola	Tipo de cable.
1000	RJ45	Rollover
1600	RJ45	Rollover
2500	RJ45	Rollover
2600	RJ45	Rollover
2600	RJ45	Rollover
4000	DB25F	Straight-through Serial
4500	DB25F	Straight-through Serial
4700	DB25F	Straight-through Serial
7000	DB25F	Straight-through

7200	DB25F	Serial Straight-through Serial
7500	DB25F	Straight-through Serial
12000	DB25F	Straight-through Serial

Tabla 12.2.1 Tipos de conectores del puerto de consola para diferentes series de enrutadores Cisco.

- **Puerto serial asíncrono (TTY.)**

El puerto serial asíncrono también conocido como TTY, tiene las mismas características físicas que el puerto de consola, y es usado para acceso dial-up a través de un modem usando PPP (Point to Point Protocol), o SLIP (Serial Line Internet Protocol) a través de una línea serial remota. Este tipo de puerto no todos los enrutadores lo tienen, sino que depende del modelo del mismo.

- **Puerto auxiliar (AUX.)**

El puerto auxiliar tiene las mismas características físicas que el puerto de consola, la mayoría de los enrutadores tiene un puerto auxiliar, el cual igual que el puerto de consola nos permite comunicarnos con el enrutador tanto en forma local como remota.

El puerto auxiliar es frecuentemente usado para la conexión de un módem para administración del enrutador "out-of-band" o fuera de banda. Un camino "out-of-band" no lleva paquetes enrutados, es usado primariamente para acceder a un enrutador cuando una ruta de red o circuito falla.

- **Puertos virtuales (VTY.)**

Son líneas de terminal lógicas (Virtual TeleTypes), usadas para acceso al enrutador a través de la aplicación Telnet. El acceso físico es a través de cualquiera de las interfaces de red del mismo.

Son referidos comúnmente como VTY's, y cada enrutador puede tener varios puertos virtuales, por default se tienen 5 TTYs, pero se pueden quitar o agregar más, dependiendo de cuántos se necesite tener.

### 12.3 Acceso local.

Cuando un equipo es nuevo o no está configurado podemos comunicarnos con él únicamente a través de su puerto de consola ya que las interfaces del enrutador no están activas aún.

Para realizar la conexión local, se debe considerar primero la conexión física y luego la conexión lógica.

La conexión física se hace entre el puerto de consola y la terminal de consola o el puerto serial del equipo terminal usado para acceder al enrutador, usando para ello cable serial.

Si conectamos una terminal de consola al puerto de consola del enrutador, habilitamos la comunicación con el mismo. La terminal puede ser una terminal tonta ASCII como la vt100 o una computadora personal (PC.)

Si usamos una computadora personal como terminal debemos tener software de emulación de terminal ejecutándose en la PC, e introduciendo comandos en el teclado podemos hacer que el IOS del enrutador los ejecute.

Las computadoras personales usualmente tienen dos puertos seriales, el primero es comúnmente un conector DB9 macho (DB9M) pero algunas otras tienen un conector DB25M.

Para los enrutadores que tienen un conector RJ45, el cable "roll over" es generalmente suministrado con el equipo, además de al menos un adaptador, el cual permite conectarlo al puerto serial de la terminal.

Si la terminal tiene un conector DB9M en el puerto serial, se usa el adaptador RJ45 a DB9F (Hembra.)

Si la terminal tiene un conector DB25M en el puerto serial, se usa el adaptador RJ45 a DB25F (Hembra.)

Para los enrutadores que tengan un conector de consola DB25F, estos no traen el cable que se necesita, sino que uno mismo debe de proveerse de él.

Este cable debe tener un conector DB25M en una punta, y en la otra el conector apropiado para el puerto de la terminal de consola.

El cable debe de estar configurado en "straight through", es decir que los hilos deben de tener las puntas finales con las mismas asignaciones.

En capítulos anteriores se describió la construcción del cable rollover.

Como se mencionó anteriormente, si la terminal a ser usada es una PC, ésta debe tener software de emulación de terminal para poder interactuar con el IOS del enrutador.

Este software simula las capacidades de una terminal para transmitir información desde el teclado y recibirla en la pantalla. Debe decirse que el procesamiento es realizado por el enrutador, ya que es en él donde esta ejecutándose el sistema operativo de red.

El software de emulación de terminal puede ser obtenido de firmas comerciales o como otro tipo de distribución. Básicamente todos tienen las mismas funciones, mas algunas otras que sirven para poder hacer más fácil su uso.

Si la terminal de consola es ASCII, no hay necesidad de ejecutar software especial, solo hay que verificar que la configuración de la terminal sea la misma que espera el enrutador.

### 12.3.1 Uso de Hyperterminal o de otros programas de emulación de terminal para conectarse a un equipo Cisco a través del puerto de consola.

Esto se hace a través del puerto de consola tal como ya se dijo. El software Hyperterminal es más conocido y utilizado ya que viene incluido con el sistema operativo MS Windows, además de que el funcionamiento de otros emuladores es similar al de Hyperterminal.

Primero se ejecuta el programa emulador de terminal, en este caso Hyperterminal.

Después de que el programa se ha ejecutado aparecerá una ventana que deberemos llenar con los datos correctos.

Se elige un nombre para la conexión (por ejemplo Cisco) para hacer referencia la configuración que se usara cada que se conecte a un equipo.

Luego seleccionamos un puerto para comunicarnos con el COM1 o COM2 dependiendo de cual puerto serial esté disponible, y lo configuramos para que pueda establecer comunicación con el puerto de consola. La configuración por defecto en el puerto de consola Cisco es la siguiente:

9600 bps.
8 bits de datos.
Sin paridad.
1 BIT de parada.
Control por hardware.



En el caso de que el enrutador tenga una configuración diferente a la original se debe usar la misma para nuestro puerto serial.

Después de esto nos conectamos al puerto de consola del enrutador y con ello al IOS. En ocasiones es necesario pulsar ENTER para que nos responda.

### 12.4 Acceso remoto.

Al igual que la conexión local, la conexión remota se compone de la conexión física y de la conexión lógica. La conexión física se hace a través de cualquiera de las interfaces de red activas del enrutador, o a través de los puertos locales como el serial asíncrono o el puerto auxiliar, conectando un módem que permita hacer la llamada desde otro lugar.

Para el acceso a las interfaces de red, solamente es necesario tener acceso a cualquiera de las redes en las que el enrutador está conectado.

El tipo de acceso remoto es el más viable y cómodo, cuando los equipos están dispersos o muy alejados del sitio donde se está trabajando, ya que no se necesita estar físicamente junto al enrutador, aunque también tiene la desventaja de que no se pueden realizar maniobras en sitio como cambiar conexiones físicas, cableado, etc.

---

Para la conexión remota es necesario que el enrutador esté activo y conectado a la misma red donde está la terminal o host desde el que se quiere acceder o que sí están en diferentes redes, que haya un punto de acceso en el cual ambas redes pueden intercambiar datos.

La conexión a través de los puertos seriales o auxiliares por marcado remoto se realiza usando protocolos seriales como SLIP y PPP y el acceso se realiza a través de la aplicación Telnet.

Para este tipo de acceso se necesita tener el enrutador con la configuración mínima para poder aceptar accesos remotos.

Entre esta configuración mínima están las direcciones de red de cada interfaz, el nombre de host, cuentas y passwords, la pila de protocolos TCP/IP ejecutándose a fin de soportar todas las funciones necesarias, etc.

Cuando la conexión física se hace a través de las interfaces de red activas, la conexión lógica se hace a través de las terminales virtuales que mantiene el IOS del enrutador.

El acceder a los enrutadores a través de la red o interred puede ser hecho usando la aplicación Telnet para establecer una conexión a una de las terminales virtuales del enrutador remoto (VTY's.)

La aplicación Telnet solo puede ser hecha a través de redes y hosts corriendo IP, por lo tanto es necesario que el enrutador esté ejecutando esta pila de protocolos. El host puede ser una estación de trabajo, una PC u otro enrutador que pueda ejecutar el Telnet y que tenga conectividad IP.

Para hacerlo solo se necesita ejecutar el comando que lance el Telnet usando como argumento la dirección IP o el nombre del enrutador remoto al que se quiere acceder.

Para el caso de usar el nombre del equipo remoto en vez de su dirección IP, el equipo local debe realizar el proceso de resolución de dirección antes de poder hacer la conexión al equipo remoto, ya que es necesario saber la dirección IP del host destino.

Hay dos maneras de realizar la resolución de dirección:

- Tabla de hosts local.

Ésta es una tabla almacenada en el equipo local, que contiene entradas para los nombres y direcciones IP de equipos remotos conocidos.

Generalmente es editada manualmente y es útil solo si son pocos equipos de los que se pretende hacer referencia por el nombre, además de que éstos deben de usar IP's estáticas y no dinámicas.

- Servicio de nombre de dominio. (DNS)

DNS es una aplicación que corre en un servidor. El servidor acepta una petición conteniendo el nombre de un host y busca en sus tablas la dirección IP del equipo referido. Una vez que lo encuentra regresa la dirección IP al equipo que hizo la solicitud. De no ser así trata de localizarlo en la red y si no puede, responde que no puede traducir la dirección.

Una vez recibida la dirección IP, el equipo local puede entonces hacer la conexión al equipo remoto.

Para poder realizar la resolución de nombres, el equipo debe tener configurada la dirección IP del equipo servidor de nombres, de no ser así y si no logra encontrar uno en la red, entonces no es posible traducir el nombre a una dirección IP y por tanto no se puede hacer la conexión remota.

Aunque se ha mencionado que el acceso se realiza a través de Telnet; como se verá más adelante en el esquema de conexión propuesto, se utilizará una variante llamada Reverse Telnet, la cuál será descrita a detalle posteriormente.

Actualmente en el mundo de la seguridad en informática, la aplicación Telnet está siendo desplazada por otra llamada SSH (Secure Shell) o Shell seguro, la cual además de las mismas características funcionales de Telnet, provee mecanismos de seguridad que evitan que los comandos y los passwords enviados entre ambos equipos sean en texto plano sin ningún tipo de cifrado o mecanismo de seguridad de los datos.

SSH (Secure Shell) es un programa para conectarse a otros equipos a través de una red abierta en forma segura, para ejecutar comandos en una máquina remota y para mover archivos de una máquina a otra. Proporciona una exhaustiva autenticación y comunicaciones seguras en redes no seguras"

SSH provee fuerte autenticación y comunicación segura sobre un canal inseguro y nace como un reemplazo a los comandos Telnet, ftp, rlogin, rsh, y rep, los cuales proporcionan gran flexibilidad en la administración de

una red, pero sin embargo, presenta grandes riesgos en la seguridad de un sistema. Adicionalmente, ssh provee seguridad para conexiones de servicios X Windows y envío seguro de conexiones arbitrarias TCP.

Secure Shell admite varios algoritmos de cifrado entre los cuales se incluyen:

- Blowfish
- 3DES
- IDEA
- RSA

La ventaja más significativa de ssh es que no modifica mucho las rutinas. En todos los aspectos, iniciar una sesión de ssh es tan similar y sencillo como iniciar una sesión de Telnet. Tanto el intercambio de llaves, la autenticación, así como el posterior cifrado de sesiones son transparentes para los usuarios. Sin embargo se requiere que ambos equipos puedan soportarlo, lo cuál no es posible debido a las características de los enrutadores que vamos a utilizar, pero si es posible utilizarlo si así se desea entre los equipos terminales como estaciones de trabajo y servidores.

### 12.5 Esquema de conexión propuesto.

En este apartado se propone un esquema de conexión entre una terminal y los equipos que facilite la operación del laboratorio.

El esquema es ilustrado en la figura siguiente:

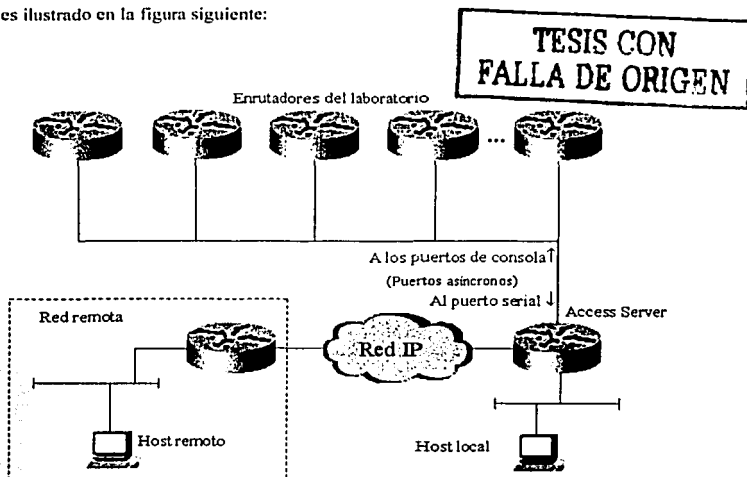


Figura 12.5.1 Esquema de conexión propuesto para las el acceso local y remoto.

Este esquema propone que el acceso a cualquiera de los enrutadores designados para estar disponibles local o remotamente, se realice a través de un solo equipo o un solo punto, que en este caso será un enrutador que estará conectado desde un puerto serial asíncrono a cada uno de los puertos de consola de los enrutadores

---

referidos anteriormente. Dicho enrutador se le llamará Access Server. También estará conectado a la red local y a la red externa. Con esto se consigue que desde un punto local o remoto se pueda tener acceso a este enrutador y desde él, acceder a los demás enrutadores.

En este esquema se combinan tanto el acceso local como remoto, ya que el acceso aunque se puede hacer desde otros equipos se realiza a través del puerto de consola de los enrutadores. Para ello se necesita que el Access Server disponga de una dirección IP a través de la cual se puede acceder a él.

Como se menciono anteriormente la característica que permite al Access Server funcionar como el enlace entre los puertos de consola de los equipos y las terminales desde las que se quiere realizar la conexión es el Reverse Telnet.

Un Access Server no es más que un enrutador con múltiples puertos asíncronos de baja velocidad que pueden ser conectados directamente a otros dispositivos seriales, como módems o puertos de consola de otros enrutadores, a través de Reverse Telnet.

Reverse Telnet permite hacer una conexión de Telnet de regreso al dispositivo desde el que se realizó la solicitud sobre una interfaz diferente.

Los comandos de configuración para habilitar Reverse Telnet en el Access Server son los siguientes:

Los enrutadores Cisco no aceptan conexiones entrantes a los puertos asíncronos (TTYs) por default. Para que la o las líneas acepten conexiones entrantes se tienen que especificar uno o varios protocolos de transporte. Para ello se usa el comando siguiente en modo de configuración de línea, que fuerza a que cualquier dato que es enviado a ellas por el enrutador sea enviado de salida por el mismo puerto, y cualquier dato que es recibido en ellas, sea pasado directamente a las conexiones a tal puerto.

***NombreEnrutador(config-line)#transport input all***

Cualquier puerto de línea de un enrutador Cisco, puede ser direccionado por el correspondiente número de puerto. Dichos número de puerto empiezan en el 2001 y hacia arriba. El primer puerto, es decir el 2001 se refiere a la línea 1, el 2002 se refiere a la línea 2 y así sucesivamente hasta la última línea que se haya configurado para recibir conexiones con el comando anterior (transport input all)

Después de que los números de puertos son asignados, el puerto AUX obtiene el último número de puerto, es decir que si se tienen 8 puertos de línea el AUX tendrá el 2009

De esta manera si se realiza una conexión desde un enrutador o estación de trabajo al Access Server con una dirección IP 10.1.1.1 como la siguiente, se podrá acceder a la línea 1 del Access Server.

***NombreEnrutador>telnet 10.1.1.1 2001***

Frecuentemente la dirección IP de la interfaz Loopback es elegida para realizar la conexión dado que esta nunca se cae y esta disponible mientras haya conectividad por cualquiera de las interfaces físicas del enrutador, a diferencia de una interfaz física que si se cae, se pierde la conectividad con el equipo aunque este tenga otras interfaces aun activas.

Para crear una interfaz de Loopback se utiliza el comando en modo de configuración global siguiente:

***NombreEnrutador(config)#interface loopback {numero\_de\_interfaz}***

Dicho comando hace que se entre en el modo de configuración de interfaz de Loopback, donde podemos asignar la dirección IP a dicha interfaz como con cualquier otro tipo de interfaz física.



---

Si se tiene un problema de conexión cuando se trata de acceder a un equipo se puede usar el comando siguiente para limpiar la línea deseada.

*AccessServer #clear line {numero\_de\_linea}*

Una vez que se ha hecho la conexión Telnet a otro dispositivo, se necesita la capacidad de regresar a la sesión al Access Server para hacer conexiones a otros dispositivos o regresar a otras sesiones ya abiertas. Para regresar al Access Server se necesita presionar la secuencia de teclas [control-shift-6] + [x], una vez en él se pueden ver las sesiones activas con el comando:

*AccessServer#show sessions*

Se puede regresar a una sesión abierta desde el Access Server presionando el número de sesión y luego Enter.

No se debe olvidar configurar un password Telnet, ya que de ser así no se podrá ser capaz de realizar la conexión Telnet desde ningún lugar.

*AccessServer(config)#line vty 0 4*

*AccessServer(config-line)#password {password}*

Se puede configurar al enrutador a hacer una conexión Telnet a cualquier host con el comando siguiente:

*AccessServer(config)#ip host {nombre\_de\_host} [Puerto\_TCP] {direccion\_IP\_del\_host}*

Dicho comando define un nombre estático para hacer un mapeo de nombre-dirección en la caché de hosts del enrutador, lo cual es aplicable a Telnet y Reverse Telnet.

## 12.6 Resumen.

La conexión a los equipos provee el medio adecuado para poder interactuar con ellos, lo cual es la base de la práctica que se pueda adquirir en el uso del laboratorio.

Se deben de comprender las diferentes maneras en que se realiza la conexión y comunicación con los equipos del laboratorio, ya sea de forma local y remota.

Los procedimientos para poder interactuar con el IOS del enrutador no son vistos aquí, pero básicamente son como en cualquier otro sistema operativo de línea de comandos, en el que para poder ingresar se realizan procedimientos de autenticación y autorización para poder ejecutar las diferentes tareas que el IOS del enrutador puede realizar.

El uso del acceso local o remoto debe de ser hecho de acuerdo a requerimientos específicos, ya que cada uno tiene diferentes ventajas y desventajas, tanto en la funcionalidad que pueden proporcionar, como en la facilidad de uso, los problemas que pueden y no pueden solucionar, etc.

Para el laboratorio que vamos a implementar se planea que se pueda tener tanto el acceso local como el remoto, por lo que se debe de configurar el mismo con los lineamientos ya mencionados para poder lograrlo.

**TESIS CON  
FALLA DE ORIGEN**

---

## Capítulo 13.

### 13 Protocolos y tecnologías a soportar por el laboratorio.

#### 13.1 Introducción.

En este capítulo se da un breve listado de las tecnologías y protocolos que se pretenden soportar en el laboratorio, y que estarán disponibles para poder usarlos en las prácticas y cursos que se pretenden dar en el laboratorio. Algunas de estas tecnologías no serán soportadas aun debido a que no se cuenta con el hardware adecuado para poderse implementar, pero se prevé que a futuro se pueda adquirir lo necesario para hacerlo. A continuación se enlistan las tecnologías y protocolos que se planean utilizar en el laboratorio, ordenados por su ubicación en el modelo de referencia OSI. Así como un breve resumen de lo que son y lo que hacen. El detalle de las tecnologías mencionadas se encuentra explicado en la primera parte de la tesis.

#### 13.2 Protocolos y tecnologías de capa 1 y 2 del modelo de referencia OSI.

En esta parte se consideran las tecnologías ubicadas en la capa 1 y 2 del modelo de referencia OSI.

##### IEEE 802.2.

Es un protocolo LAN de la IEEE que especifica una implementación de la subcapa LLC de la capa de enlace de datos. IEEE 802.2 maneja errores, entramados, control del flujo y la interfaz de servicio de la capa de red o capa 3. Se utiliza en las LAN IEEE 802.3 e IEEE 802.5.

##### Ethernet.

Ethernet es una tecnología LAN de capas 1 y 2 desarrollada por Digital, Intel y Xerox (DIX.) Opera a 10 Mbps y usa CSMA/CD como método de acceso al medio. Ethernet es una tecnología LAN muy común dada su simplicidad de operación y de implementación.

Esta tecnología y sus variantes son las más fáciles de implementar y las más usadas.

Esta tecnología se planea implementarla en el laboratorio desde el principio.

##### IEEE 802.3.

IEEE 802.3 es un protocolo LAN de la IEEE que especifica la implementación de la capa física y de la subcapa MAC de la capa de enlace de datos. IEEE 802.3 utiliza el acceso CSMA/CD a varias velocidades a través de diversos medios físicos. Las extensiones del estándar IEEE 802.3 especifican implementaciones para Fast Ethernet. Las variaciones físicas de la especificación IEEE 802.3 original incluyen 10Base2, 10Base5, 10BaseF, 10BaseT y 10Broad36. Las variaciones físicas para Fast Ethernet incluyen 100BaseTX y 100BaseFX.

Algunas de estas extensiones de IEEE 802.3 serán implementadas en el laboratorio de acuerdo al hardware poseído.

##### Token Ring.

Token Ring es una tecnología LAN de capa 1 y 2, que transmite a 4 y 16 Mbps haciendo uso de tokens. Fue desarrollado originalmente por IBM en 1970 y fue una tecnología popular antes de que Ethernet se volviera más popular y la reemplazara.

##### IEEE 802.5.

Es un protocolo LAN de la IEEE, que especifica la implementación de la capa física y la subcapa MAC de la capa de enlace de datos. IEEE 802.5 usa acceso de transmisión de tokens a 4 ó 16 Mbps en cableado STP o UTP y desde el punto de vista funcional y operacional es equivalente a Token Ring de IBM.

Tanto la implementación de Token Ring como la de IEEE 802.5 están ya en desuso, y siendo reemplazadas por Ethernet y otras tecnologías más modernas. Sin embargo, se planea implementar esta tecnología ya que contaremos con el hardware adecuado.

#### FDDI (Fiber Distributed Data Interface.)

---

**FDDI** es un estándar de LAN que usa un anillo de fibra óptica dual, accede al medio usando token-passing y opera a 100 Mbps. Es frecuentemente usado como tecnología de Backbone por su alto ancho de banda y por cubrir mayores distancias que el cobre. Se planea contar desde un principio con hardware para implementar FDDI.

**ISDN (Integrated Services Digital Network.)**

Es un protocolo de comunicaciones que ofrecen las compañías telefónicas y que permite que las redes telefónicas transmitan datos, voz y tráfico de otros orígenes. Fue la evolución a las redes digitales de la antigua red telefónica pública conmutada. Actualmente se sigue utilizando pero es una tecnología ya vieja.

**SDLC (Synchronous Data Link Control.)**

SDLC es un protocolo de comunicaciones de capa de enlace de datos de SNA. SDLC es un protocolo serial full-dúplex orientado a bit que ha dado origen a numerosos protocolos similares, entre ellos HDLC y LAPB.

**LAPB (Link Access Procedure Balanced.)**

Protocolo de capa de enlace de datos en la pila de protocolo X.25. LAPB es un protocolo orientado a bit derivado de HDLC.

**HDLC (High-Level Data Link Protocol.)**

HDLC es un protocolo síncrono de la capa de enlace de datos o capa 2, orientado a bit, desarrollado por la ISO. HDLC especifica un método de encapsulamiento de datos en enlaces seriales síncronos que utiliza caracteres de trama y sumas de comprobación.

**PPP (Point to Point Protocol.)**

PPP es un protocolo WAN de capa 2, provee un método estándar para transportar datagramas multiprotocolo sobre enlaces punto a punto. PPP es capaz de operar a través de cualquier interfaz DTE/DCE. PPP no impone ninguna restricción acerca de la tasa de transmisión más que la impuesta por la interfaz DTE/DCE en particular

**Frame Relay.**

Frame Relay es un protocolo WAN de alto desempeño que opera en las capas uno y dos del modelo de referencia OSI. Frame Relay es la evolución de X.25 y opera sobre diferentes interfaces físicas.

**ATM (Asynchronous Transfer Mode.)**

Estándar internacional para conmutación de celdas en el que varios tipos de servicios (por ejemplo, transmisión de voz, video o datos) se transmiten en celdas de longitud fija (53 bytes.) Las celdas de longitud fija permiten que el procesamiento de las celdas se produzca en el hardware, reduciendo así los retardos de tránsito. ATM se encuentra diseñado para aprovechar los medios de transmisión de alta velocidad como E3, SONET y T3.

Inicialmente no contaremos con el hardware necesario para implementar ATM, pero se prevé que en el futuro así sea.

**13.3 Protocolos de capa 3 y 4 del modelo de referencia OSI.**

Con los enrutadores en el laboratorio y los IOS cargados en ellos, se pueden usar diferentes protocolos de capas 3 y 4, sin embargo, por el momento solo nos centraremos en los que están relacionados con IP o más específicamente con la suite de TCP/IP.

Existen otras suites de protocolos propietarios como AppleTalk y Novell IPX, los cuales son menos usados que IP. Pero dada la vastedad de TCP/IP no sería posible abarcar todos ellos en un solo curso por lo que no se consideran inicialmente.

En un futuro se podrían considerar como materia de estudio, ya que su implementación es solo cuestión de habilitarlos en los enrutadores.

---

La Suite TCP/IP es la pila de protocolos de comunicación de datos más común y difundida, sobre la cual corren la mayoría de las aplicaciones y servicios existentes. Esta pila consta de varios protocolos, cada uno con sus respectivas funciones, y que en conjunto logran transmitir la información de un lugar a otro. Todos estos protocolos son cargados en el IOS de los enrutadores o el OS de los hosts cuando se indica instalar la pila TCP/IP.

#### **IP (Internet Protocol.)**

IP es un protocolo de capa 3 que se encarga del transporte de los datos de un punto a otro de la red, actualmente se usa la versión 4 (IPv4) pero ya se está planeando la migración a la nueva versión (IPv6.) IP es un protocolo no orientado a conexión ya que esta tarea está destinada a otros protocolos de capas superiores.

#### **ARP (Address Resolution Protocol.)**

ARP es un protocolo de capa 2 que se encarga de resolver las direcciones de la capa de red a direcciones de capa de enlace. Es decir, resuelve las direcciones IP a direcciones MAC.

#### **InARP (Inverse Address Resolution Protocol.)**

Realiza el mapeo de direcciones de capa 3 a direcciones de capa 2 en redes sin capacidad de broadcast como Frame Relay.

#### **ICMP (Internet Control Messaging Protocol.)**

ICMP es un protocolo cuya función es la de enviar mensajes de control sobre el estado de la red y su tráfico.

#### **RARP (Reverse Address Resolution Protocol.)**

RARP es un protocolo que se encarga de hacer el proceso inverso que ARP. Es decir, que resuelve direcciones IP a partir de la dirección MAC.

#### **UDP (User Datagram Protocol.)**

UDP es un protocolo de capa 4 o capa de transporte, que se encarga de controlar el transporte de los paquetes IP de un punto a otro de la red, sin asegurarse de la entrega de los mismos y dejando esta tarea a otros protocolos en capas superiores.

#### **TCP (Transfer Control Protocol)**

TCP es un protocolo de capa 4 o capa de transporte, que se encarga de controlar el transporte de los paquetes IP en forma confiable y orientada a conexión.

### **13.4 Protocolos de enrutamiento IP.**

En esta parte se consideran los protocolos de enrutamiento para IP. Esto es necesario porque los enrutadores necesitan un método para construir sus tablas de enrutamiento para poder hacer las decisiones de reenvío de paquetes IP.

Existen varios protocolos de enrutamiento para IP, cada uno con sus características y ventajas propias. El conocer los diferentes protocolos de enrutamiento existentes y su funcionamiento es importante para poder elegir el más apropiado.

#### **RIP v1 (Routing Information Protocol version 1.)**

RIP v1 es un protocolo de vector distancia, es el más simple que existe, y es apropiado para redes pequeñas. Sin embargo, no soporta CIDR, VLSM, rutas paralelas ni redes discontinuas.

#### **RIP v2 (Routing Information Protocol version 2.)**

RIP v2 es un protocolo de vector distancia que supera algunas de las limitaciones que tiene RIP v1. Las mejoras con respecto a RIP v1, son que RIP v2 es capaz de usar VLSM y, por tanto, enrutar entre redes discontinuas.

---

### **IGRP (Interior Gateway Routing Protocol.)**

IGRP es otro protocolo de vector distancia, que puede tomar para calcular la métrica a más variables que la simple cuenta de saltos como lo hace RIP, e incluye el ancho de banda, el delay, etc. Debido a su mejor manejo de métrica puede enrutar correctamente entre enlaces redundantes y caminos paralelos. Sin embargo, no es capaz de enrutar entre redes discontinuas ya no que no soporta VLSM.

Tampoco tiene la limitación de 15 saltos como la tenía RIP, ya que permite hasta 255 saltos, lo cual permite redes más grandes.

### **EIGRP (Enhanced Interior Gateway Routing Protocol.)**

EIGRP es la versión mejorada desarrollada por Cisco de IGRP. Este protocolo ofrece propiedades de convergencia y eficacia operativa superiores a otros protocolos de enrutamiento, y combina las ventajas de los protocolos de estado de enlace, con las ventajas de los protocolos de vector distancia.

### **OSPF (Open Shortest Path First.)**

OSPF es un protocolo de enrutamiento de estado de enlace, puede operar en redes muy grandes con características de enlaces redundantes, es classless, balancea cargas y soporta VLSM. Por ser de estado de enlace consume poco ancho de banda, aunque requiere procesadores con alto desempeño ya que requiere ejecutar algoritmos complejos para realizar el proceso de convergencia.

### **IS-IS (Intermediate System - Intermediate System.)**

Es un protocolo de enrutamiento jerárquico de estado de enlace basado en el enrutamiento DECnet Fase V, en el que los IS (enrutadores) intercambian información de enrutamiento con base en una métrica única para determinar la topología de la red.

### **BGP (Border Gateway Protocol.)**

Protocolo de enrutamiento entre sistemas autónomos que reemplaza a EGP. BGP intercambia información de accesibilidad con otros sistemas BGP. La versión actual es la 4.

BGP es el protocolo de enrutamiento interdominio más ampliamente usado en Internet, soporta CIDR y usa mecanismos de agregación de rutas para reducir el tamaño de las tablas de enrutamiento.

## **13.5 Protocolos y servicios de capas superiores (4, 5 y 6) del modelo de referencia OSI.**

Entre las aplicaciones de capas superiores se encuentran una gran cantidad de protocolos y especificaciones estándar y propietarias. Cada una realiza tareas específicas para el trabajo en red, la facilidad de configuración de la red y la administración de la misma. Entre las más importantes están los siguientes:

### **DHCP (Dynamic Host Configuration Protocol.)**

DHCP es un protocolo para configurar dinámicamente las direcciones IP de los equipos de una red, lo que permite mayor facilidad de administración y escalabilidad de la red.

### **Telnet**

Telnet es una aplicación incluida en la suite de TCP/IP que corre sobre conexiones TCP. Permite establecer conexiones remotas similares a las de consola con lo que es posible realizar las mismas tareas que si se estuviera frente al equipo.

### **NAT (Network Address Translation.)**

NAT es una función que realiza la traducción entre direcciones de una red IP por las de otra. Es usado comúnmente para conectar una red privada con la red pública con el fin de economizar direcciones IP públicas.

### **FTP (File Transfer Protocol.)**

FTP es un protocolo que sirve para transferir archivos de un lugar a otro de la red con mayor eficiencia que con otros métodos.

---

### **CDP (Cisco Discovery Protocol.)**

Es un protocolo de descubrimiento que corre en todos los equipos fabricados por Cisco, que incluyen enrutadores, servidores de acceso, puentes y conmutadores. Usando CDP, un equipo puede advertir la existencia de otros equipos en la misma LAN o en el lado remoto de una WAN. Se ejecuta en todos los medios que soportan SNAP incluyendo LAN, Frame Relay y ATM.

### **RMON (Remote MONitoring.)**

Remote Monitoring (RMON) es una especificación de monitoreo que permite habilitar varios monitores de red y sistemas de consola para intercambiar datos de monitoreo de red.

RMON identifica la actividad en los nodos individuales y permite supervisar todos los nodos y su interacción en un segmento de LAN. Usado junto con SNMP en un enrutador, RMON permite ver tanto el tráfico que fluye por el enrutador como el que hay en el segmento.

### **SNMP (Simple Network Management Protocol.)**

SNMP es un protocolo de gestión de red, permite a un servidor TCP/IP que ejecuta una aplicación SNMP, interrogar a otros nodos para obtener estadísticas y condiciones de error de la red. Los otros servidores, que proporcionan agentes SNMP responden a estas preguntas y le permiten a un solo servidor recoger estadísticas de muchos nodos de la red.

### **DNS (Domain Name System.)**

DNS es un sistema con el cual se realiza la resolución de nombres que son fáciles de entender y recordar por el usuario, por direcciones IP entendibles por los equipos de una red IP.

### **WINS (Windows Internet Name Service)**

WINS es un protocolo parecido a DNS, diseñado para redes que usan NetBIOS, y que proporciona funciones agregadas para esos sistemas.

### **Protocolos para correo electrónico.**

Entre los servicios de Internet que necesitamos se requiere el de correo electrónico. Existen varios protocolos para administrar el correo que pueden ser elegidos para configurarse en el servidor y los clientes. Los más importantes son los siguientes:

- **SMTP (Simple Mail Transfer Protocol)**

SMTP es un protocolo de capas superiores que usa datagramas TCP para transporte y es usado como protocolo para transportar correo electrónico de manera confiable.

- **POP3 (Post Office Protocol version 3.)**

Es un protocolo para la gestión de correo en Internet. Es el más utilizado junto con SMTP. POP3 no está destinado a proveer de extensas operaciones de manipulación de correo sobre el servidor; normalmente, el correo es transmitido y entonces borrado. Funciona como cliente / servidor, y es el que permite que los mensajes queden almacenados en el servidor hasta que el usuario revise su casilla de correo con un programa cliente de e-mail y descargue los mensajes

- **IMAP4 (Internet Message Access Protocol rev 4)**

IMAP es un protocolo diseñado para permitir la manipulación de buzones remotos como si fueran locales. IMAP requiere de un servidor que haga las funciones de oficina de correos pero en lugar de leer todo el buzón y borrarlo, solicita sólo los encabezados de cada mensaje. Se pueden marcar mensajes como borrados sin suprimirlos completamente, pues estos permanecen en el buzón hasta que el usuario confirma su eliminación

### **Servicios de capa de presentación y de sesión.**

Los servicios de presentación y sesión proporcionan la base para que las aplicaciones funcionen. En ocasiones se presentan como API's de programación o en forma de bibliotecas disponibles en los sistemas operativos en los que se está trabajando.

---

Los más importantes son los siguientes:

- **Sockets.** Es un API de capa de sesión, que esta integrado al kernel de BSD UNIX. Winsocks o Sockets de Windows corre sobre sistemas que usan la pila TCP/IP de Microsoft. Es una versión de la de BSD hecha por Microsoft y otros desarrolladores de software y generalmente se implementa en forma de DLLs con programas adicionales.

- **RPC (Remote procedure Calls)** las llamadas de procedimiento remoto son un método para ejecutar programas o procedimientos en otros nodos de red de manera que parecen ejecutarse localmente. Las RPC están ubicadas en las capas de sesión y de presentación. Un estándar del mecanismo RPC es el Distributed Computing Environment (DEC RPC) al que se ajustan HP, IBM y Microsoft.

- **NetBIOS** es un API de capa de sesión y no un protocolo, se encuentra en ambientes Windows o Microsoft. NetBIOS puede correr sobre diversos protocolos; sobre TCP/IP se describe en la RFC 1001/2 y puede usar UDP o TCP como protocolos de transporte. Las aplicaciones escritas con la API NetBIOS generalmente necesitan mas información que la que proporciona DNS, por eso Microsoft desarrollo Windows Internet Name Service o WINS que provee la capacidad de registrar dinámicamente nombres a través de subredes IP lógicas, es decir después de dar saltos a través de los enrutadores. Un buen entendimiento de NetBIOS es crítico en cualquier red que use Microsoft LAN Manager o Windows NT como sistema operativo de red. NetBIOS también puede operar con IPX o NetBEUI además de TCP/IP. Los programas de aplicación usan NetBIOS para comunicaciones cliente / servidor o de igual a igual.

### 13.6 Resumen.

En este capítulo se listaron las tecnologías y protocolos que se pretenden usar en el laboratorio en función de los equipos con los que se planea contar a corto y a largo plazo. Aunque en un principio no se cuente con el hardware necesario se da un adelanto de lo que se visualiza tener a futuro en el laboratorio.

Se debe recalcar que la lista aquí presentada puede y debe extenderse conforme se requiera para mantener el laboratorio al tanto de las nuevas tecnologías que se desarrollen en el mundo de las redes.

Además, una de las funciones del laboratorio es la de experimentar con nuevas tecnologías y protocolos y su interacción entre ellos. Las únicas limitaciones son en cuanto al hardware que es más caro y difícil de obtener, pero en lo que se refiere a software y protocolos se tienen menos limitantes ya que estos son más fáciles de obtener.

---

## **Capítulo 14**

### **Ejemplos de prácticas sugeridas para el laboratorio.**

#### **14.1 Introducción.**

En este capítulo se darán algunos ejemplos de prácticas que pueden ser llevadas a cabo en el laboratorio, aunque no pretenden ser incluidas tal como están en las prácticas definitivas de la materia, ya que tal tarea debe ser llevada a cabo por la coordinación de laboratorios correspondiente. Sin embargo sirven de ejemplo de lo que se puede realizar.

#### **14.2 Prácticas de ejemplo.**

##### **14.2.1 Protocolo de enrutamiento EIGRP.**

###### **Protocolo de enrutamiento EIGRP.**

###### **Objetivo:**

Configurar los equipos de una red con el protocolo de enrutamiento EIGRP, verificar su operación y su funcionamiento.

###### **Antecedentes.**

Los antecedentes teóricos deben de ser proporcionados en la clase de teoría. Y se encuentran también en la primera parte de esta tesis.

###### **Equipamiento necesario:**

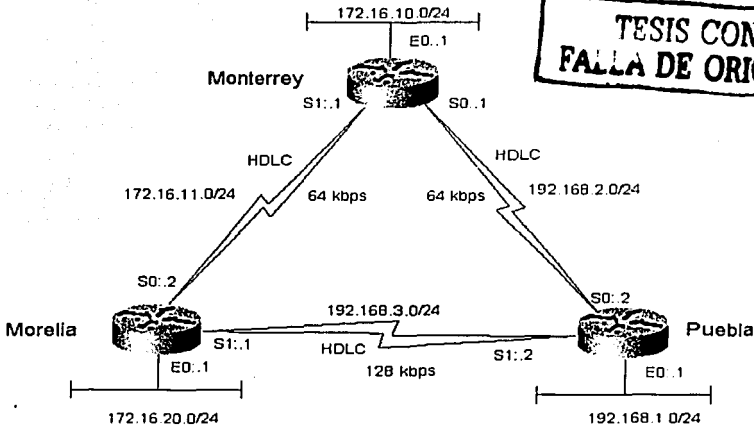
- Tres enrutadores Cisco 2500. (Cisco IOS 10.0 o superior)
- Una PC corriendo software de emulación de terminal.
- Tres cables V.35 DTE/DCE para conexiones seriales.
- Cables rolled.

###### **Procedimiento.**

Para esta práctica se utilizará la red mostrada en el siguiente diagrama.



# TESIS CON FALLA DE ORIGEN



- El primer paso es armar físicamente la red y realizar las conexiones mostradas.
- El siguiente paso es configurar el IOS de los enrutadores involucrados. Para ello se utilizan los datos mostrados en el diagrama anterior.  
Se deberán configurar:
  - Los nombres de host.
  - Las interfaces de cada enrutador y sus direcciones IP.
  - El protocolo de enrutamiento EIGRP en todas las interfaces.
- El último paso es verificar el funcionamiento del protocolo EIGRP y realizar pruebas de conectividad.

Una vez que la red está completamente configurada, y el protocolo de enrutamiento EIGRP ejecutándose, se puede verificar su funcionamiento con los siguientes comandos.

**NombreEnrutador>show ip protocols**

Es un comando muy útil para obtener información general acerca de cuáles protocolos de enrutamiento IP están corriendo, y como están configurados, en este caso solo el proceso EIGRP es el que nos interesa.

Podemos ver cuales son los enrutadores vecinos (aquellos corriendo EIGRP con el mismo ASN) con el comando:

**NombreEnrutador>show ip eigrp neighbors**

Este comando también nos proporciona información de las interfaces configuradas con el protocolo, las direcciones IP y los contadores "hold" y "uptime" usados por EIGRP.

Si queremos ver la tabla de topología de EIGRP usamos el comando:

*Nombre Enrutador>show ip eigrp topology*

- Para realizar pruebas de conectividad entre los segmentos se colocan dispositivos terminales como estaciones de trabajo en los diferentes segmentos y se pueden utilizar comandos como ping y tracer para verificar el envío de paquetes correcto entre ellos.

El archivo running-config y startup-config deben de ser muy similar las configuraciones mostradas:

#### Enrutador monterrey

```
!
version 11.2
no service udp-small-servers
no service tftp-small-servers
!
hostname monterrey
!
interface E0
ip address 172.16.10.1 255.255.255.0
no shutdown
interface s0/1
ip address 192.168.2.1 255.255.255.0
clockrate 64000
no shutdown
!
interface s1
ip address 172.16.11.1 255.255.255.0
clockrate 64000
no shutdown
!
router eigrp 110
network 172.16.0.0
network 192.168.0.0
no auto-summary
!
line con 0
login
line aux 0
line vty 0 4
login
!
```

TESIS CON  
FALLA DE ORIGEN

#### Enrutador morelia

```
!
version 11.2
no service udp-small-servers
no service tftp-small-servers
```

```
!
hostname morelia
!
interface E0
ip address 172.16.20.1 255.255.255.0
no shutdown
!
interface s0
ip address 172.16.11.2 255.255.255.0
clockrate 64000
no shutdown
!
interface s1
ip address 192.168.3.1 255.255.255.0
clockrate 128000
no shutdown
!
router eigrp 110
network 172.16.0.0
network 192.168.0.0
no auto-summary
!
line con 0
login
line aux 0
line vty 0 4
login
!
```

170  
170  
170  
170  
170

TESIS CON  
FALLA DE ORIGEN

#### Enrutador puebla

```
!
version 11.2
no service udp-small-servers
no service tcp-small-servers
!
hostname puebla
!
interface E0
ip address 192.168.1.1 255.255.255.0
no shutdown
!
interface s0
ip address 192.168.2.2 255.255.255.0
clockrate 64000
no shutdown
!
interface s1
ip address 192.168.3.2 255.255.255.0
clockrate 128000
```

**TESIS CON  
FALLA DE ORIGEN**

```
no shutdown
!  
router eigrp 110  
network 172.16.0.0  
network 192.168.0.0  
no auto-summary  
!  
line con 0  
login  
line aux 0  
line vty 0 4  
login  
!
```

Pueden agregarse más ejercicios que sirvan para mostrar más de las características de EIGRP.

#### 14.2.2 Listas de acceso IP estandar.

##### Objetivo.

Configurar los equipos de una red simple de muestra con listas de acceso IP estándar, verificar su operación y su funcionamiento.

##### Antecedentes.

Los antecedentes teóricos deben de ser proporcionados en la clase de teoría. Y se encuentran también en la primera y segunda parte de esta tesis.

##### Equipamiento necesario:

- Dos enrutadores Cisco 2500. (Cisco IOS 10.0 o superior)
- Una PC corriendo software de emulación de terminal.
- Un cable V.35 DTE/DCE para conexiones seriales.
- Un cable rolled.

##### Introducción.

Las listas de acceso IP son colecciones secuenciales de proposiciones que permiten o niegan el tráfico de una dirección IP específica o un rango de ellas.

El enrutador chequea las direcciones IP en el paquete entrante o saliente por la interfaz especificada y las compara una por una a las especificadas en cada proposición de la lista de acceso, hasta encontrar una coincidencia explícita, momento en el cual realizara la acción configurada.

El orden de las proposiciones en la lista de acceso es crítico dado que la primera coincidencia es la que se toma en cuenta.

Tampoco se debe olvidar que implícitamente en cada lista de acceso hay una proposición que filtra y desecha cada paquete que no haya sido permitido expresamente en la lista de acceso.

##### Procedimiento.

Esta configuración demuestra el filtrado de paquetes usando listas de acceso estándar. La figura siguiente muestra el esquema de conexión que se utilizara.

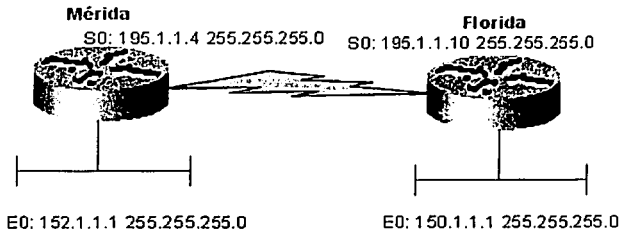


Figura 14.2.2 Esquema de conexión.

TESIS CON  
FALLA DE ORIGEN

Se debe cumplir con lo siguiente:

- El enrutador Mérida permitirá todo el tráfico proveniente de la red 150.1.1.0 y negará el tráfico de cualquier otra red.
- El enrutador Mérida y el enrutador Florida están conectados serialmente
- El enrutador Florida actuará como DCE suministrando el reloj al enrutador Mérida.
- Cada enrutador conoce las rutas a cada una de las redes existentes por medio de algún protocolo de enrutamiento o rutas estáticas.
- Las direcciones IP están asignadas como se muestra en la figura.
- El enrutador Florida tiene configurada una dirección LoopBack (151.1.1.1) a manera de punto de prueba.
- Una lista de acceso de entrada será aplicada a la interfaz serial del enrutador Mérida, permitiendo paquetes desde la red 150.1.1.0; todos los demás paquetes de otras redes serán filtrados.
- El enrutador Florida hará pings a la interfaz serial del enrutador Mérida (195.1.1.4) usando el comando ping extendido para varias la dirección IP fuente de direcciones IP múltiples.

- a) El primer paso es armar físicamente la red y realizar las conexiones mostradas.
- b) El siguiente paso es configurar el IOS de los enrutadores involucrados. Para ello se utilizan los datos mostrados en el diagrama anterior.

Se deberán configurar en caso de no estarlo:

- c) Se deben configurar las listas de acceso IP estándar mencionadas.
- d) El último paso es verificar el funcionamiento del filtrado de paquetes IP con el comando ping extendido y realizar pruebas de conectividad.

El archivo running-config y startup-config deben de ser muy similar las configuraciones mostradas:

#### Enrutador Mérida

```

version 11.2
no service udp-small-servers
  
```

UNIVERSIDAD DE MERIDA  
FACULTAD DE INGENIERIA  
CARRERA DE INGENIERIA EN SISTEMAS DE COMPUTACION

TESIS CON  
FALLA DE ORIGEN

```
no service tcp-small-servers
!
hostname merida
!
interface E0
ip address 152.1.1.1 255.255.255.0
no shutdown
no keepalive
!
interface s0
ip address 195.1.1.4 255.255.255.0
no shutdown
!
router eigrp 110
network 152.1.0.0
network 195.1.0.0
no auto-summary
!
access-list 1 permit 150.1.1.0 0.0.0.255
!
line con 0
login
line aux 0
line vty 0 4
login
!
```

Enrutador florida

```
!
version 11.2
no service udp-small-servers
no service tcp-small-servers
!
hostname florida
!
interface E0
ip address 150.1.1.1 255.255.255.0
no shutdown
no keepalive
!
interface s0
ip address 195.1.1.10 255.255.255.0
clockrate 64000
no shutdown
!
router eigrp 110
network 152.1.0.0
network 195.1.0.0
no auto-summary
!
line con 0
```

```
login
line aux 0
line vty 0 4
login
!
```

### Monitoreo y verificación de la configuración.

Una vez que la red esta completamente configurada, y las listas de acceso IP creadas y aplicadas, se puede verificar su funcionamiento con los siguientes comandos.

#### *NombreEnrutador#ping*

Esto nos permitirá entrar a las opciones del comando ping extendido (se debe estar en el modo Privileged EXEC), y para hacer las pruebas se pueden usar direcciones IP fuente de las diferentes redes a las que el enrutador esta conectado. Se puede saber si la conexión fue exitosa o fallida con los símbolos desplegados por el comando al ejecutarse, tal como se vio en la descripción del comando dentro del a tesis.

Como ejemplo:

#### *Florida#ping*

*Protocol[IP]:*

*Target IP address: 195.1.1.4*

*Repeat count[5]:*

*Datagram size[100]:*

*Timeout in seconds[2]:*

*Extended commands[n]:y*

Source address or interface: 151.1.1.1

Type of Service[0]:

Set DF bit in IP header?[no]:

Validate Reply data?[no]:

Data Pattern[0xABCD]:

Loose, Strict, Record, TimeStamp, verbose[none]:

Sweep Range of sizes[n]:

TESIS CON  
FALLA DE ORIGEN

Se pueden monitorear los paquetes entrantes al enrutador Mérida usando el comando siguiente:

#### *merida#debug ip packet*

Se pueden ver las listas IP configuradas con el comando:

#### *merida#show ip access-list*

### 14.3 Resumen.

Estas prácticas de ejemplo no pretenden dar el formato final de las prácticas que se impartirán en el laboratorio, ya que ésta tarea corresponde a las coordinaciones y profesores correspondientes, pero sirven de muestra de lo que se puede realizar con los conocimientos adquiridos en la teoría del laboratorio y los equipos e instalaciones que se han descrito a lo largo de toda esta tesis.

---

## Capítulo 15. Administración del laboratorio.

### 15.1 Servicios del laboratorio.

A continuación se describen brevemente los servicios que se planean brindar a través del laboratorio de datos:

- Laboratorio normal para la materia "Redes de Teleinformática" y materias relacionadas que surjan en el futuro.
- Laboratorio Abierto para prácticas de materias autorizadas.
- Laboratorios Virtuales o remotos desde los cuales se puedan realizar algunas prácticas.
- Cursos en redes de datos.
- Elaboración de Manuales de prácticas para las materias autorizadas, y que contempla además el diseño y actualización de prácticas del laboratorio local y laboratorios virtuales.
- Investigación continua de nuevas tecnologías.
- Portal Web, el cual realizará la difusión de información de tecnologías y protocolos usados en redes de datos, la difusión de servicios al público en general y de los laboratorios en sitio y remotos. Así como la reservación de los demás servicios que se presten en el laboratorio.
- Laboratorio de investigación y pruebas de nuevas tecnologías.
- Asesoría en redes de datos.

### 15.2 Reglamento de uso en sitio y vía remota

El laboratorio debe de contar con un reglamento interno que regule tanto el uso en sitio como el uso remoto.

Se deben de crear políticas de uso cuyos fines sean los siguientes:

- Proteger la integridad física de los usuarios en sitio. Este es un objetivo común a cualquier instalación donde se congreguen personas. Por lo que deben existir reglamentos generales que seguir para poder modificarlos y adaptarlos al laboratorio. Se deben considerar las características propias de los dispositivos tal como se han manejado dentro de la tesis.

- Proteger la integridad física de los equipos que pertenezcan al laboratorio de daños accidentales y ocasionados.

Los lineamientos generales de cómo diseñar el laboratorio para evitar que se usen incorrectamente se han manejado a través de varios capítulos.

- Establecer políticas de uso, acceso y utilización de los servicios y recursos del laboratorio por vía remota.

Este es tal vez el objetivo más difícil de planear y de cumplir, ya que existe una gran variedad de situaciones en las que se puede poner el riesgo los servicios y recursos en el laboratorio; tanto accidentalmente como deliberadamente.

Se deben revisar caso por caso y realizar correcciones continuamente en las políticas de uso y auditoría de los accesos remotos.

- Evitar que con los recursos del laboratorio se realicen acciones indebidas que pongan en riesgo la seguridad o recursos de sistemas informáticos externos.
- Promover el uso correcto y aprovechamiento al máximo de los equipos. Con esto se busca aprovechar al máximo las posibilidades que nos brindan los equipos con los que se cuenta y evitar situaciones accidentales por falta de precaución o pericia.
- Establecer sanciones en caso de que se realicen actos que vayan en contra de los lineamientos anteriores.



---

Estas pueden ir desde la suspensión del servicio hasta la remisión a instancias superiores dentro de la jerarquía de la Universidad.

La elaboración de este o estos reglamentos están fuera del alcance de esta tesis, por lo que no se detallarán más a fondo, simplemente se dan los lineamientos generales que se consideran importantes para ello. Probablemente este reglamento sea realizado por los departamentos correspondientes de la Facultad de Ingeniería, que están encargados de las labores administrativas.

### **15.3 Inventario de equipo**

El inventario de equipo debe de realizarse para poder tener un control completo de los recursos con los que se cuenta, sin embargo dado que no es posible hacerlo hasta que se implemente y termine el laboratorio, y dado que es labor de otros departamentos no se detallará más.

### **15.4 Conclusiones.**

La elaboración de los reglamentos para administrar y operar el laboratorio están fuera del alcance de esta tesis, por lo que no se detallarán más a fondo, simplemente se dan los lineamientos generales que se consideran importantes para ello.

Estos reglamentos serán realizados por los departamentos y coordinaciones correspondientes de la Facultad de Ingeniería.

---

## Capítulo 16. Conclusiones Generales.

El trabajo de que se ha realizado en esta tesis, ha tratado de establecer las mejores guías de diseño e implementación para la construcción de un laboratorio de datos para la Facultad de Ingeniería, en ella se han tratado de cubrir todos los aspectos para la construcción y operación del mismo, sin embargo no fue posible realizar la implementación del mismo por motivos fuera de nuestro alcance.

El diseño del laboratorio y sus objetivos pueden ser aún más ambiciosos en sus alcances, pero esto de realizará con el tiempo, cuando se cuenten con más recursos y cuando los servicios que se presten de inicio en el mismo, no sean suficientes y deban expandirse. De cualquier manera el diseño realizado tiene en cuenta la posibilidad de ampliar todos los servicios.

En lo que se refiere a la parte técnica, se trató de abarcar y explicar lo mejor posible todos los aspectos que se consideran importantes para la construcción del laboratorio, sin embargo se tiene conciencia que no son suficientes y que muy probablemente se deba de recurrir a consultar documentación actualizada de otras fuentes.

En lo que se refiere a la parte administrativa, no fue el objetivo de esta tesis dedicarse a ella, aunque se dieron algunos lineamientos generales que se consideran necesarios para poder armonizar el trabajo técnico con el administrativo. Dicho trabajo administrativo deberá ser tratado por las personas que se encarguen de tales tareas dentro del organigrama que tiene la Facultad de Ingeniería y sus diversos departamentos.

La estructura de la tesis se dividió en dos partes principales. La primera parte de la tesis se enfocó a dar un repaso de la mayoría de los requerimientos teóricos que son necesarios como base para poder hacer el diseño del laboratorio. Sobre todo dar un repaso general a los modelos que son usados para comprender el funcionamiento de las tecnologías actuales, mismas que también son revisadas en esa parte. De la misma manera se clasificaron las tecnologías y protocolos de acuerdo a su funcionamiento en el modelo de referencia OSI de redes de datos.

La segunda parte de la tesis es precisamente donde se realiza el diseño del laboratorio, desde los aspectos elementales de adecuación del lugar, selección de muebles y cableado, pasando por la selección de equipos, la disposición física y lógica de los equipos de manera que estos puedan operar correctamente y sean de fácil acceso y uso por parte de los futuros usuarios.

Se describen también en esta parte de la tesis, varias propuestas para la conexión local de los equipos del laboratorio y la conexión a Internet.

Se contemplan también los servicios que se deseen prestar, con un esquema de seguridad para preservar los equipos, recursos y servicios bajo el menor riesgo posible y mantenerlos funcionando de lo mejor manera.

Como parte del acceso local a los equipos de comunicaciones, se plantea también un esquema de conexión centralizado de consolas, lo cual es indispensable ya que siempre es necesario conectarse e iniciar sesión en un equipo para poder configurarlo o monitorear su actividad en la red. De igual manera se propone un esquema de conexión para poder acceder a los equipos local y remotamente y que se complementa con los esquemas propuestos de conexión a Internet y de seguridad propuestas anteriormente.

Por último se presentan un par de prácticas de ejemplo, que reflejan los objetivos de diseño del laboratorio. En ellas ya se aprovecha toda la infraestructura diseñada con anterioridad y permite concentrarse en aspectos mas simples enfocados a mostrar o a poner en practica algún tipo de tecnología o configuración específica.

En la parte final se encuentra un glosario con los términos más importantes utilizados a lo largo de la tesis, así como la lista bibliográfica y de referencia que se utilizó para documentar esta tesis.

**Glosario de términos usados.**

<b>ABM (Asynchronous Balanced Mode)</b>	Modo de asíncrono balanceado. Un modo de comunicación HDLC (protocolos derivados) que soporta comunicaciones orientadas a punto a punto entre dos estaciones donde cualquiera puede iniciar la transmisión.
<b>Analizador de protocolos</b>	Dispositivo de control de la red que mantiene información estadística con respecto al estado de la red y de cada dispositivo conectado a ella. Las versiones más sofisticadas que usan inteligencia artificial pueden detectar, definir y solucionar los problemas de la red.
<b>Ancho de banda</b>	Diferencia entre las frecuencias más altas y más bajas disponibles para las señales de red. El término se utiliza también para describir la medida de capacidad de un medio o protocolo de red dados.
<b>ANSI (American National Standards Institute)</b>	Instituto nacional americano de normalización. Organización voluntaria compuesta por corporaciones, el gobierno y otros miembros, que coordinan actividades relacionadas con estándares, aprueba normas nacionales de EE.UU., y desarrolla posiciones para Estados Unidos en organizaciones internacionales de estándares. ANSI contribuye a desarrollar normas estadounidenses e internacionales relacionadas, entre otras cosas, con comunicaciones y networking. ANSI es miembro de IEC y de ISO.
<b>API (Application Programming Interface)</b>	Una API es una interfaz de programación de aplicaciones, una colección de comandos de programación (frecuentemente llamadas interfaces) que pueden invocar a las funciones de un programa. Algunos programas pueden utilizar sus APIs para solicitar servicios o comunicarse con un programa. Por ejemplo, el Windows 95 contiene un API conocido como el win32 API. Para que una aplicación solicite un servicio del Windows 95 lo tendrá que hacer utilizando un API win32.
<b>ARP (Address Resolution Protocol)</b>	Protocolo de resolución de direcciones. Es un protocolo que se encarga de encontrar la correspondencia entre una dirección IP y su correspondiente dirección MAC
<b>ASCII (American Standard Code for Information Interchange)</b>	Código normalizado americano para el intercambio de información. Código de 8 bits para representación de caracteres (7 bits más paridad).
<b>ATM (Asynchronous Transfer Mode)</b>	ATM se basa en el concepto de Comutación Rápida de Paquetes (Fast Packet Switching) en el que se supone una fiabilidad muy alta a la tecnología de transmisión digital, típicamente sobre fibra óptica, y por lo tanto la no necesidad de recuperación de errores en cada nodo.
<b>ATM (Asynchronous Transfer Mode)</b>	Modo de transferencia asíncrono. Es un protocolo estándar internacional para comutación de celdas en el que varios tipos de servicios se transmiten en celdas de longitud fija (53 bytes.) Las celdas de longitud fija permiten que el procesamiento de las celdas se produzca en el hardware, reduciendo así los retardos de tránsito. ATM se encuentra diseñado para aprovechar los medios de transmisión de alta velocidad como E3, SONET y T3.
<b>AUI (Attachment Unit Interface)</b>	Interfaz de unidad de conexión. Interfaz IEEE 802.3 entre una MAU y una NIC (Network Interface Card). El término AUI también se puede referir al puerto del panel posterior con el cual se podría conectar un cable AUI.
<b>Backbone</b>	La parte de una red que actúa como ruta primaria para el tráfico que sale y llega de otras redes con mayor frecuencia.
<b>Banda ancha</b>	En terminología de telecomunicaciones, cualquier canal que tenga un ancho de banda mayor que un canal con grado de voz (4 kHz). En terminología LAN, un cable coaxial sobre el cual se utiliza señalización analógica. También llamada banda amplia
<b>Banda base</b>	Característica de una tecnología de red donde se utiliza sólo una frecuencia portadora. Ethernet es un ejemplo de red de banda base. También llamada banda estrecha.
<b>BECN (Backward Explicit Congestion Notification)</b>	Notificación de la congestión explícita hacia atrás. Conjunto de bits de una red Frame Relay en las tramas que viajan en dirección opuesta a las tramas que encuentran una ruta congestionada. Los DTE que reciben las tramas con el conjunto de bits BECN pueden pedir que los protocolos de mayor nivel tomen una acción de control de flujo según corresponda.
<b>BGP (Border Gateway Protocol)</b>	Protocolo de Gateway de Borde. Es un protocolo de enrutamiento exterior muy usado en Internet.

<b>Bit</b>	Es la unidad o símbolo base de los sistemas de comunicaciones binarias.
<b>Bps (bits per second)</b>	Bits por Segundo.
<b>BRI (Basic Rate Interface)</b>	Interfaz de acceso básico. Interfaz ISDN compuesta por dos canales B y un canal D para la comunicación por circuito conmutado de voz, video y datos.
<b>Bridge (puente)</b>	Dispositivo de red que conecta dos LAN's y remite o filtra paquetes de datos entre ellas, según sus direcciones de destino. Los puentes operan al nivel de enlace de datos (o capa MAC) del modelo de referencia OSI, y es transparente a los protocolos y a los dispositivos de niveles más altos como los enrutadores.
<b>Broadcast (emisión)</b>	Paquete de datos que se enviará a todos los nodos de una red. Los paquetes o tramas broadcasts se identifican por medio de direcciones de broadcast específicas a cada tipo de direcciones.
<b>Browser</b>	Es un programa que nos permite visualizar los contenidos de la World Wide Web y desarrollar una lectura hipertextual. Parece ser que el término se originó con la aparición de la Web cuando la gente denominaba así a la interfaz que le permitía ver archivos de texto en línea. No hay que olvidar que browse es un término en inglés que significa dar un vistazo. Asimismo se conoce que el primer browser con interface gráfica fue el Mosaic inventado en 1992. A este browser o navegador como también se le conoce en nuestro idioma le siguió el Netscape navigator y finalmente el Internet Explorer.
<b>Buffer</b>	Área de almacenamiento empleada para el manejo de los datos en tránsito. Los buffers se utilizan en internetworking para compensar las diferencias en la velocidad de procesamiento entre los dispositivos de red. Las ráfagas de datos pueden almacenarse en buffers hasta tanto puedan ser manejadas por dispositivos de procesamiento más lentos. A menudo denominado buffer de paquetes.
<b>Bus</b>	Ruta de señal física común compuesta por cables u otros medios a través de los cuales pueden enviarse señales de una parte a otra de la computadora. También llamada autopista.
<b>Byte</b>	Término empleado para referirse a una serie de dígitos binarios consecutivos sobre los cuales se opera como una unidad (por ejemplo, un byte de 8 bits).
<b>Cable coaxial</b>	Cable que consta de un conductor cilíndrico exterior hueco que envuelve a un único alambre conductor interno. En las LANs se utilizan normalmente dos tipos de cable coaxial, cable de 50 ohms que se utiliza para la señalización digital, y cable de 75 ohms que se utiliza para la señal analógica y la señalización digital de alta velocidad.
<b>Cable de fibra óptica</b>	Medio físico capaz de conducir una transmisión de luz modulada. Comparado con otros medios de transmisión, el cable de fibra óptica es más costoso, pero no es susceptible a la interferencia electromagnética, y es capaz de mayores velocidades de datos. Llamado a veces fibra óptica.
<b>Canal</b>	Una ruta de comunicación. En ciertos ambientes pueden multiplexarse varios canales por un cable único.
<b>Canaleta</b>	Es un canal plástico, que protege el cable de tropiezos y rupturas, dando además una presentación estética al cableado interno.
<b>CCITT (Consultative Committee for International Telegraph and Telephone)</b>	Comité de consultoría internacional para telefonía y telegrafía. Organización internacional responsable del desarrollo de normas de comunicación. Actualmente denominada ITU-T.
<b>CDP (Cisco Discovery Protocol)</b>	Es un protocolo de descubrimiento de la red propietario de Cisco y que corre en equipos del mismo fabricante. Sirve para que un equipo pueda saber que a equipos está conectado sin necesidad de otros protocolos.
<b>CHAP</b>	Challenge Handshake Authentication Protocol. Esquema de autenticación para PPP donde la contraseña no sólo se exige al empezar la conexión sino también se requiere durante la conexión - el fallo para proporcionar la contraseña correcta durante el login o el desafío producirá la desconexión.
<b>Checksum</b>	Método para verificar la integridad de los datos transmitidos. Un checksum es un valor entero calculado a partir de una secuencia de octetos tomados por medio de una serie de operaciones aritméticas. El valor se calcula en el extremo receptor y comparado para la verificación.

<b>Checksum del encabezado</b>	Campo dentro de un datagrama IP que indica la verificación de integridad en el encabezado.
<b>CIDR(Classless Inter Domain Routing)</b>	Es un mecanismo desarrollado para ayudar a aliviar el problema del agotamiento de direcciones IP y el crecimiento de las tablas de enrutamiento. Para enfrentar este problema se desarrollo el esquema de Direcciones sin Clase, que consiste en asignar a una misma organización un bloque continuo de direcciones de Clase C.
<b>CIR (Committed Information Rate)</b>	Velocidad de información suscrita. La velocidad a la cual una red Frame Relay acuerda transferir la información bajo condiciones normales, promediadas según un incremento de tiempo mínimo. CIR, medido en bits por segundo, es una de las métricas clave negociadas de tarifa.
<b>Circuito</b>	Ruta de comunicaciones entre dos o más puntos.
<b>Circuito virtual</b>	Circuito lógico creado para garantizar una comunicación confiable entre dos dispositivos de red. Un circuito virtual se define por medio de un par VPI/VCI, y puede ser permanente (PVC) o conmutado (SVC). Los circuitos virtuales se utilizan en Frame Relay y en X.25.
<b>Closet de comunicaciones</b>	Es el lugar físico donde se concentra la infraestructura dedicada a telecomunicaciones.
<b>Codificación</b>	1. Proceso por el cual los bits son representados por tensiones. 2. Técnicas eléctricas utilizadas para transportar señales binarias.
<b>Código de detección de errores</b>	Código que puede detectar errores de transmisión mediante un análisis de los datos recibidos, basándose en la adherencia de los datos a pautas estructurales apropiadas.
<b>Cola</b>	1. En general, una lista de elementos ordenada a la espera de ser procesada. 2. En enrutamientos, una reserva de paquetes que esperan ser enviados por una interfaz de enrutador.
<b>Colisión</b>	En Ethernet, el resultado de dos nodos transmitiendo en forma simultánea. Las tramas provenientes de cada dispositivo impactan y se dañan al encontrarse en el mismo medio físico.
<b>Conector DB</b>	Conector de bus de datos. Tipo de conector utilizado para conectar cables en serie y paralelos a un bus de datos. Los nombres del conector DB son de formato DB-x, donde x representa el número de (cables) dentro del conector. Cada línea se conecta a un pin del conector, pero en muchos casos, no todos los pins tienen asignada una función. Los conectores DB se definen por diferentes normas EIA/TIA.
<b>Conector RJ (Registered Jack)</b>	Conector tipo ficha registrado. Conectores estándar normalmente empleados para conectar las líneas telefónicas. Los conectores RJ se utilizan actualmente para las conexiones telefónicas y 10BaseT como así también para otros tipos de conexiones de red. RJ-11, RJ-12, y RJ-45 son algunos de los tipos de conectores RJ más difundidos.
<b>Configuración balanceada</b>	En HDLC, una configuración de red punto a punto con dos estaciones combinadas.
<b>Configuración básica</b>	Información de configuración mínima que se ingresa cuando se instala en la red un nuevo enrutador, switch u otro dispositivo de red configurable.
<b>Configuración no balanceada</b>	Configuración de HDLC con una estación primaria y múltiples estaciones secundarias.
<b>Congestión</b>	Tráfico que excede la capacidad de una red.
<b>Commutación de circuitos</b>	Sistema de conmutación en el cual debe existir una ruta dedicada de circuito físico entre el emisor y el receptor durante la duración de la llamada.
<b>Commutación de mensajes</b>	Técnica de conmutación que consiste en la transmisión de mensajes de nodo a nodo por una red. El mensaje se almacena en cada nodo hasta que esté disponible una ruta de envío.
<b>Commutación de paquetes</b>	Técnica de conmutación de paquetes en la cual las tramas son procesados por completo antes de salir por el puerto correspondiente. Este procesamiento incluye el cálculo de CRC y la verificación de la dirección de destino. Además, las tramas deben almacenarse temporalmente hasta que los recursos de la red (por ejemplo un enlace no utilizado) estén disponibles para enviar el mensaje.
<b>Control de errores</b>	Técnica utilizada para detectar y corregir errores en transmisiones de datos.
<b>Control de paridad</b>	Proceso para verificar la integridad de un carácter. Una verificación de paridad involucra la colocación de un BIT que hace que el número total de dígitos 1 binarios en un carácter o "word" (excluyendo al bit de paridad) tanto impar (para paridad impar) como par (para

	paridad par).
<b>Convergencia</b>	Velocidad y capacidad de recuperación de un grupo de dispositivos de red que corren un protocolo de enrutamiento que sufren un cambio o falla en la topología establecida (volver a establecer el enlace).
<b>CRC (Cyclic redundancy check)</b>	Verificación por redundancia cíclica. Técnica de verificación de errores en la que el receptor de la trama calcula un resto dividiendo el contenido de una trama por un divisor binario primo y compara el resto calculado con un valor almacenado en la trama por el nodo emisor.
<b>CSMA/CD (Carrier sense multiple access with collision detection)</b>	Acceso múltiple con detección de portadora y detección de colisiones. Mecanismo de acceso al medio en el cual los dispositivos listos para transmitir datos primero verifican que el canal este libre, si el medio de transmisión se encuentra libre un dispositivo puede transmitir. Si dos dispositivos transmiten a la vez, tiene lugar una colisión y ésta es detectada por todos los dispositivos que entran en colisión. En consecuencia, la colisión demora las retransmisiones desde dichos dispositivos por un lapso al azar. El acceso CSMA/CD es utilizado por Ethernet e IEEE 802.3.
<b>CSU (Channel service unit)</b>	Unidad de servicio de canal. Dispositivo de interfaz digital que conecta el equipamiento del usuario final al bucle telefónico digital local. Frecuentemente denominado conjuntamente con DSU como CSU/DSU.
<b>Datagrama</b>	Agrupamiento lógico de información enviada como una unidad de capa de red por un medio de transmisión sin establecer previamente un circuito virtual. Los datagramas IP son las unidades principales de información en Internet. Los términos frame, mensaje, paquete, y segmento también se utilizan para describir los agrupamientos lógicos de información en las diferentes capas del modelo de referencia OSI y en varios círculos de tecnología.
<b>Datos</b>	Datos del protocolo de capa superior.
<b>DCE (Data Communications Equipment)</b>	Equipo de comunicación de datos (expansión EIA) o equipo de transmisión de datos (expansión ITU-T). Los dispositivos y conexiones de una red de comunicaciones que comprenden el extremo de la red de la interfaz de usuario a red. DCE brinda una conexión física a la red, envía el tráfico y brinda una señal de sincronización utilizada para sincronizar la transmisión de datos entre los dispositivos DCE y DTE. Los módems y las tarjetas de interfaz son ejemplos de DCE.
<b>Demodulación</b>	Proceso de retornar una señal modulada a su forma original. Los módems realizan la demodulación, tomando una señal analógica y retornándola a su forma original (digital).
<b>Demultiplexación</b>	La separación de múltiples tramas de entrada que han sido multiplexadas en una señal física común, volviéndolas nuevamente a múltiples tramas de salida.
<b>Dialup</b>	(Llamar) Acción de llamar desde un módem a otro módem remoto por vía telefónica.
<b>Dirección</b>	Estructura de datos o convención lógica utilizada para identificar una entidad única, como un proceso particular o un dispositivo de red.
<b>Dirección IP</b>	Dirección de 32 bits asignada a los hosts que utilizan TCP/IP. Una dirección IP corresponde a una de cinco clases (A, B, C, D, o E) y se escribe en forma de 4 octetos separados con puntos (formato decimal con punto). Cada dirección consiste en un número de red, un número opcional de subred, y un número de host. Los números de red y de subred se utilizan conjuntamente para el enrutamiento, mientras que el número de host se utiliza para el direccionamiento a un host individual dentro de la red o de la subred. Para extraer la información de la red y de la subred de la dirección IP se utiliza una máscara de subred. También denominada dirección de Internet.
<b>Dirección MAC</b>	Dirección de la capa de enlace de datos estandarizada, necesaria para cada puerto o dispositivo conectado a una LAN. Otros dispositivos en la red utilizan estas direcciones para localizar puertos específicos en la red, y para crear y actualizar tablas de enrutamiento y estructuras de datos. Las direcciones MAC tienen una longitud de 6 bytes y son controladas por IEEE. También conocidas como dirección de hardware, dirección de capa MAC, o dirección física.
<b>DLCI (Data Link Connection Identifier)</b>	Identificador de conexión de enlace de datos. Valor que especifica un PVC o SVC en una red Frame Relay. En la especificación básica Frame Relay, los DLCI son localmente significativos (los dispositivos conectados podrían utilizar valores diferentes para especificar la misma conexión). En la especificación LMI extendida, los DLCI son globalmente significativos (los DLCI especifican dispositivos finales individuales).
<b>DTE (Data Terminal)</b>	Equipo terminal de datos. Dispositivo en el extremo usuario de una interfaz de usuario a red

<b>Equipment)</b>	que sirve como origen de datos, destino, o ambos. DTE se conecta a una red de datos a través de un dispositivo DCE (por ejemplo, un módem) y utiliza en forma típica señales de sincronización generadas por el DCE. DTE incluye dispositivos tales como computadoras, traductores de protocolo y multiplexores.
<b>E1</b>	Sistema de transmisión digital de área amplia, utilizado predominantemente en Europa, que transporta datos a una velocidad de 2,048 Mbps. Las líneas E1 se pueden arrendar de portadoras comunes para uso privado.
<b>EBCDIC (extended binary coded decimal interchange code)</b>	Código ampliado de caracteres decimales codificados en binario. Cualquiera de una variedad de conjuntos de caracteres codificados desarrollados por IBM que consisten en caracteres codificados de 8 bits. Este código de caracteres es utilizado por sistemas IBM y máquinas de télex más antiguas.
<b>EIA (Electronic Industries Association)</b>	Asociación de industrias electrónicas. Grupo que especifica las normas de transmisión eléctrica. EIA y TIA han desarrollado numerosas normas de comunicación bien conocidas, incluyendo a EIA/TIA-232 y EIA/TIA-449.
<b>EIA/TIA-232</b>	Norma común de interfaz de capa física, desarrollada por EIA y TIA, que soporta circuitos no balanceados a velocidades de señal de hasta 64 kbps. Se asemeja estrechamente a la especificación V.24. Conocida anteriormente como RS-232.
<b>EIA/TIA-449</b>	Interfaz popular de capa física desarrollada por EIA y TIA. Básicamente, una versión más rápida (hasta 2 Mbps) de EIA/TIA-232, capaz de soportar longitudes de cable más extensas. Conocida anteriormente como RS-449.
<b>EIA-530</b>	Se refiere a dos aplicaciones eléctricas de EIA/TIA-449: RS-422 (para transmisión balanceada) y RS-423 (para transmisión no balanceada).
<b>EIGRP (Enhanced Interior Gateway Routing Protocol)</b>	Es un protocolo de enrutamiento propietario de Cisco, que mejora a IGRP.
<b>E-MAIL</b>	Permite enviar y recibir mensajes desde cualquier lugar del mundo. Para eso se necesita de una casilla o dirección electrónica en la que es posible recibir cartas. También es factible anexar documentos, planillas de cálculo, sonido e imágenes.
<b>Emulación de terminal</b>	Aplicación de red en la cual una computadora corre un software que la hace aparecer ante un host remoto como una terminal conectada directamente.
<b>Encabezado</b>	Información de control colocada antes de los datos cuando se encapsulan dichos datos para la transmisión en red.
<b>Encapsulación</b>	Envoltura de datos en un encabezado de protocolo particular. Por ejemplo, los datos de Ethernet se envuelven en un encabezado específico de Ethernet antes de su tránsito por la red. Además, cuando se hace bridging de redes disímiles, se coloca simplemente todo la trama de una red en el encabezado utilizado por el protocolo de la capa de enlace de datos de la otra red.
<b>Encriptación</b>	La aplicación a los datos de un algoritmo específico para alterar la presentación de los datos al hacerlos incomprensibles para los terceros que no estén autorizados a ver la información.
<b>Enlace</b>	Canal de comunicaciones en red que consta de un circuito o ruta de transmisión y todo el equipo relativo entre un emisor y un receptor. Se lo utiliza más frecuentemente para referirse a una conexión WAN. Algunas veces denominado línea o enlace de transmisión.
<b>Enrutador</b>	Dispositivo de capa de red que utiliza una o más métricas para determinar la ruta óptima por la cual se enviará el tráfico de la red. Los enrutadores envían paquetes de una red a otra en base a la información de capa de red.
<b>Enrutamiento</b>	Proceso que consiste en encontrar la ruta hasta el host de destino. El enrutamiento es muy complejo en las redes de grandes dimensiones debido a los diversos destinos intermedios potenciales que un paquete debe atravesar antes de llegar a su host de destino.
<b>Enrutamiento dinámico</b>	Enrutamiento que se ajusta automáticamente a la topología de la red o a los cambios de tráfico.
<b>Enrutamiento jerárquico</b>	Enrutamiento basado en un sistema de direccionamiento jerárquico. Por ejemplo, los algoritmos de enrutamiento IP utilizan direcciones IP que contienen números de red, números de subred y números de host.
<b>Equilibrio de la carga (Load Balancing)</b>	En enrutamiento, la capacidad de un enrutador de distribuir el tráfico por todos sus puertos de red que se encuentren a la misma distancia de la dirección de destino. Los buenos algoritmos de balanceo de carga utilizan tanto la información sobre velocidad como sobre

	confiabilidad de la línea. El equilibrio de la carga aumenta la utilización de los segmentos de red, por lo que incrementa efectivamente el ancho de banda de la red.
<b>Estación primaria</b>	En los protocolos de capa de enlace de datos binariamente sincronizados, tales como HDLC y SDLC, una estación que controla la actividad de transmisión de las estaciones secundarias y realiza otras funciones de gestión tales como el control de error a través del sondeo u otros medios. Las estaciones principales envían comandos a las estaciones secundarias y reciben respuestas. También llamada simplemente primaria.
<b>Estación secundaria</b>	En los protocolos de capa de enlace de datos síncronos de bits, como por ejemplo HDLC, estación que responde a los comandos de una estación primaria. A menudo denominada simplemente secundaria.
<b>Estándar de facto</b>	Norma que existe por la naturaleza de su uso generalizado.
<b>Ethernet</b>	Especificación de LAN de banda base, inventada por Xerox Corporation y desarrollada conjuntamente por Xerox, Intel, y Digital Equipment Corporation. Las redes Ethernet utilizan CSMA/CD y corren por una variedad de tipos de cable a 10 Mbps. Ethernet es similar a la serie de normas IEEE 802.3.
<b>FDDI (Fiber Distributed Data Interface)</b>	Interfaz de datos distribuida por fibra. Norma LAN, definida por ANSI X3T9.5, que especifica una red de token-passing de 100-Mbps que utiliza un cable de fibra óptica, con distancias de transmisión de hasta 2 km. FDDI utiliza una arquitectura de anillo doble para dar redundancia.
<b>FECN (Forward Explicit Congestion Notification)</b>	Notificación explícita de la congestión hacia adelante. Bit colocado por una red Frame Relay para informar al DTE que recibe la trama que se ha producido una congestión en la ruta del origen al destino. El DTE que recibe las tramas con el bit FECN colocado puede solicitar que protocolos de mayor nivel tomen las medidas apropiadas para controlar el flujo.
<b>Filtrado de tráfico local</b>	Proceso por el cual un bridge filtra (descarta) tramas cuyas direcciones MAC origen y destino están ubicadas en la misma interfaz en el bridge, evitando así que el tráfico innecesario sea enviado a través del bridge. Definido en el estándar IEEE 802.1.
<b>Fragmentación</b>	Proceso de dividir un paquete en unidades más pequeñas cuando se transmite por un medio de red que no puede soportar el tamaño original del paquete.
<b>Fragmento</b>	Parte de un paquete más grande que ha sido dividido en unidades más pequeñas.
<b>Frame Relay</b>	Protocolo de la capa de enlace de datos conmutados, que administra varios circuitos virtuales. Frame Relay es más eficaz que X.25, el protocolo para el cual se considera por lo general un reemplazo.
<b>Freeware</b>	Tipo de licencia de uso en la que el programador que creó la aplicación o código fuente permite que cualquiera la pueda usar sin esperar retribución alguna, pero con la condición de no modificar el código.
<b>FTP (File Transfer Protocol)</b>	Protocolo de transferencia de archivos.
<b>Full Duplex</b>	Capacidad para la transmisión simultánea de datos entre una estación transmisora y una estación receptora.
<b>GNU</b>	Fundación para el Software Libre. Busca eliminar las restricciones de uso, copia, modificación y distribución del software. Actualmente se encuentra apoyando el desarrollo de sistemas operativos (Linux), compiladores (compilador GNU C Compiler (gcc), Perl), etc. Trata de promover, desarrollar y usar del software libre en todas las áreas de la computación. Específicamente, la Fundación pone a disposición de todo el mundo un completo e integrado sistema de software llamado GNU. La mayor parte de este sistema está ya siendo utilizado y distribuido. El costo del software únicamente esta determinado por el costo del material utilizado para distribuirlo
<b>Half duplex</b>	Capacidad de transmisión de datos solamente en una dirección a la vez, entre una estación de envío y una estación de recepción.
<b>Hardware</b>	Todo aquel dispositivo electrónico tangible.
<b>HDLC (High-Level Data Link Control)</b>	Control de enlace de datos de alto nivel. Protocolo de la capa de enlace de datos, orientado a bit y síncrono desarrollado por ISO. Proveniente de SDLC, HDLC especifica un método de encapsulación de datos sobre enlaces en serie síncronos que utilizan caracteres de trama y checksums.
<b>Hexadecimal</b>	Base 16. Una representación numérica que utiliza los dígitos 0 a 9, con su significado usual, más las letras A a F para representación de los dígitos hexadecimales con valores de 10 a 15.



	El dígito ubicado más a la derecha cuenta unos, el siguiente cuenta múltiplos de 16, por lo tanto $16^2=256$ , etc.
Host	Sistema de computación en una red. Similar al término nodo excepto que el host usualmente implica un sistema de computación, mientras que un nodo generalmente se aplica a cualquier sistema en red, incluyendo los servidores de acceso y enrutadores.
HTML	Hypertext Markup Language. Lenguaje en que se escriben los documentos que se utilizan en Internet.
HTTP (Hyper Text Transfer Protocol)	Protocolo de comunicación entre clientes y servidores Web.
Hub (concentrador)	Es un dispositivo que trabaja en la capa 1 del modelo de referencia OSI, que distribuye un mensaje en la red en forma de broadcast por todos sus puertos. <ol style="list-style-type: none"> <li>En forma general, un término utilizado para describir un dispositivo que sirve como centro de una red de topología en estrella.</li> <li>Dispositivo de hardware o software que contiene múltiples módulos independientes pero conectados de equipo de red e internetwork. Los hubs pueden ser activos (cuando repiten señales enviadas a través de ellos) o pasivos (cuando no repiten, sino que meramente dividen las señales enviadas a través de ellos).</li> <li>Ethernet e IEEE 802.3, un repetidor Ethernet multipuerto, algunas veces denominado como concentrador.</li> </ol>
ICMP (Internet Control Messaging Protocol)	Es un protocolo de la pila TCP/IP que se encarga de transmitir los mensajes de error y de control referentes a los paquetes enviados entre dispositivos.
IEEE (Institute of Electrical and Electronics Engineers)	Instituto de ingeniería eléctrica y electrónica. Organización profesional entre cuyas actividades se incluye el desarrollo de estándares para comunicaciones y redes. Los estándares IEEE para LAN son los estándares para LAN predominantes en la actualidad.
IEEE 802.12	Estándar IEEE para LAN que especifica la capa física y la subcapa MAC de la capa de enlace de datos. IEEE 802.12 emplea el esquema de acceso al medio con prioridad de demanda a 100 Mbps sobre una serie de medios físicos.
IEEE 802.2	Protocolo IEEE para LAN que especifica la implementación de la subcapa LLC de la capa de enlace de datos. IEEE 802.2 maneja errores, entramado, control de flujo y la interfaz de servicio de la capa de red (Capa 3). Se utiliza en LANs IEEE 802.3 e IEEE 802.5.
IEEE 802.3	Protocolo IEEE para LAN que especifica la implementación de la capa física y de la subcapa MAC de la capa de enlace de datos. IEEE 802.3 utiliza el acceso CSMA/CD a varias velocidades a través de diversos medios físicos. Las extensiones del estándar IEEE 802.3 especifican implementaciones para Fast Ethernet. Las variaciones físicas de la especificación IEEE 802.3 original incluyen 10Base2, 10Base5, 10BaseF, 10BaseT, y 10Broad36. Las variaciones físicas de Fast Ethernet incluyen 100BaseT, 100BaseT4, y 100BaseX.
IEEE 802.4	Protocolo IEEE para LAN que especifica una implementación de la capa física y de la subcapa MAC de la capa de enlace de datos. IEEE 802.4 utiliza un acceso token passing sobre una topología de bus y se basa en la arquitectura LAN del tipo token bus.
IEEE 802.5	Protocolo IEEE para LAN que especifica una implementación de la capa física y de la subcapa MAC de la capa de enlace de datos. IEEE 802.5 utiliza un acceso token passing a 4 Mbps sobre cableado STP y es similar al Token Ring de IBM.
IGRP (Interior Gateway Routing Protocol)	Es un protocolo de enrutamiento de vector distancia, toma en cuenta para asociar el costo a las rutas a parámetros como el ancho de banda, el retraso, etc.
Interfaz	<ol style="list-style-type: none"> <li>Conexión entre dos sistemas o dispositivos</li> <li>En terminología de enrutamiento, una conexión de red.</li> <li>Límite entre capas adyacentes del modelo OSI.</li> </ol>
Internet	Término utilizado para referirse a la mayor internetwork global que conecta a decenas de miles de redes de todo el mundo y que tiene una "cultura" que apunta básicamente a la investigación y a la estandarización basándose en el uso en la vida real. Muchas tecnologías de red líderes provienen de la comunidad de Internet. La Internet evolucionó en parte a partir de la ARPANET. Antes llamada también Internet DARPA. No debe confundirse con el término general Internet.
InterNIC	Organización que sirve a la comunidad de Internet brindando asistencia al usuario.

	documentación, capacitación, servicio de registro de nombres de dominio de Internet y otros servicios. Antiguamente llamado Network Information Center (NIC) (Centro de Información de Redes).
<b>Interoperabilidad</b>	Capacidad de equipos de computación fabricados por diferentes empresas para comunicarse entre sí exitosamente a través de una red.
<b>Intertrack</b>	Se refiere a todo aquel dispositivo instalado entre diferentes racks
<b>INTRANET</b>	Red de servicios similar a Internet, pero limitada a computadores de una sola red computacional (LAN, MAN o WAN).
<b>Intrarrack</b>	Se refiere a todo aquel dispositivo instalado en un mismo rack.
<b>IOS (Internetworking Operating System)</b>	Sistema operativo de red. Es un sistema operativo desarrollado por Cisco para administrar sus enrutadores, switches y bridges.
<b>IP (Internet Protocol)</b>	Protocolo Internet. Protocolo de capa de red de la pila TCP/IP que ofrece un servicio de internetwork sin conexión. El IP tiene prestaciones para direccionamiento, especificación del tipo de servicio, fragmentación y rearmado, y seguridad. Documentado en RFC 791.
<b>IPX (Internetwork Packet Exchange)</b>	Intercambio de paquetes en una internetwork. Protocolo de capa de red (capa 3) NetWare utilizado para transferir datos desde los servidores hacia las estaciones de trabajo. IPX es similar a IP y a XNS.
<b>ISDN (Integrated Services Digital Network)</b>	Red digital de servicios integrados. Protocolo de comunicaciones que ofrecen las empresas telefónicas y que permite que las redes telefónicas transmitan datos, voz y tráfico de otros orígenes.
<b>IS-IS (Intermediate System - Intermediate System)</b>	Protocolo de enrutamiento de estado de enlace, se basa en el modelo de referencia OSI y sirve para enlutar en redes muy grandes y complejas.
<b>ISO (International Organization for Standardization)</b>	Organización internacional para la normalización. Organización internacional que tiene a su cargo una amplia gama de estándares, incluidos aquellos referidos a networking. ISO desarrolló el modelo de referencia OSI, un popular modelo de referencia de networking.
<b>ISP (Internet Service Provider)</b>	Proveedor de servicio de Internet. Es la empresa encargada de proveer la conexión y el transporte de los datos del usuario.
<b>ITU-T (International Telecommunication Union Telecommunication Standardization Sector)</b>	Unión internacional de las telecomunicaciones (ITU-T) (ex -Comité de consultoría Internacional para telefonía y telegrafía - CCITT-). Organización internacional que desarrolla estándares de comunicación.
<b>Java</b>	Ambiente de programación simple, robusto, de propósito general, dinámico, multitareas, independiente de plataformas y orientado al objeto. Permite crear tanto aplicaciones como pequeños programas para Internet, redes internas y cualquier otro tipo de redes distribuidas.
<b>LAN (Local Area Network)</b>	Red de área local. Red de datos de alta velocidad y bajo nivel de error que cubre un área geográfica relativamente pequeña (hasta unos pocos miles de metros). Las LANs conectan estaciones de trabajo, periféricos, terminales y otros dispositivos en un único edificio u otra área geográficamente limitada. Los estándares de LAN especifican el cableado y señalización en las capas física y de enlace datos del modelo OSI. Ethernet, FDDI y Token Ring son tecnologías LAN ampliamente utilizadas.
<b>LAPB (Link Access Procedure, Balanced)</b>	Procedimiento de acceso al enlace, balanceado. Protocolo de la capa de enlace de datos de la pila de protocolos X.25. LAPB es un protocolo orientado a bit derivado de HDLC.
<b>Latencia</b>	Retraso entre el tiempo en que un dispositivo requiere acceso a la red y el tiempo en que se le da permiso para transmitir.
<b>LED (Light Emitting Diode)</b>	Diodo electroluminiscente. Dispositivo semiconductor que emite luz producida convirtiendo energía eléctrica. Las luces de estado en los dispositivos de hardware son típicamente LEDs.
<b>Línea dedicada</b>	Línea de comunicaciones que se encuentra reservada indefinidamente para transmisiones, en lugar de la conmutada que es la que se requiere en las transmisiones.
<b>Línea multipunto</b>	Línea de comunicaciones que tiene varios puntos de acceso por cable. Llamada a veces una línea "multidrop".
<b>LLC (Logical Link Control)</b>	Control de enlace lógico. La más alta de las dos subcapas de la capa de enlace de datos definida por IEEE. La subcapa LLC maneja el control de errores, el control de flujo, el entramado y el direccionamiento de subcapa MAC. El protocolo LLC que más prevalece es

	IEEE 802.2, que incluye tanto la variante sin conexión como la orientada a conexión.
<b>LMI (Logical Management Interface)</b>	Interfaz de gestión local. Conjunto de mejoras de la especificación Frame Relay básica. LMI incluye el soporte para mecanismo de actividad, que se asegura de que los datos fluyan; un mecanismo multicast, que proporciona al servidor de red su DLCI local y el DLCI multicast; direccionamiento global, que proporciona a los DLCI una significación global en lugar de local en redes Frame Relay; y un mecanismo de estado, que proporciona un constante informe de estado en los DLCI conocidos por el switch. Conocida como LMT en la terminología ANSI.
<b>MAC (Media Access Control)</b>	Control de acceso al medio. La inferior de las dos subcapas de la capa de enlace de datos definida por IEEE. La subcapa MAC administra el acceso a medios compartidos, por ejemplo, si se utilizará token passing o contención.
<b>Máscara de dirección</b>	Combinación de bits que se utiliza para describir qué porción de una dirección se refiere a la red o subred y cuál parte se refiere al host. A veces se la llama simplemente máscara.
<b>Máscara de subred</b>	Máscara de dirección de 32 bits que se utiliza en el IP para indicar los bits de una dirección IP que se están utilizando para la dirección de subred. También llamada simplemente máscara.
<b>MAU (Media attachment unit)</b>	Unidad de conexión al medio. Dispositivo utilizado en redes Ethernet e IEEE 802.3 que provee una interfaz entre el puerto AUI de una estación y el medio común de Ethernet. MAU, que puede ser creada en una estación, o que puede ser un dispositivo separado, lleva a cabo funciones de la capa física, incluso la conversión de datos digitales de la interfaz Ethernet, la detección de colisiones, y la inyección de bits en la red. Llamada a veces unidad de acceso al medio, también abreviada como MAU, o transceptor. En Token Ring, una MAU es conocida como una unidad de acceso a varias estaciones y se abrevia en general MSAU para evitar confusiones.
<b>Mensaje</b>	Agrupación lógica de información de la capa de aplicación (capa 7), a menudo compuesta por una cantidad de agrupaciones lógicas de capas inferiores, tales como paquetes. Los términos datagrama, frame, paquete, y segmento también se emplean para describir agrupaciones lógicas de información en diversas capas del modelo de referencia OSI y en diversos círculos de tecnología.
<b>Modelo de referencia OSI</b>	Modelo de referencia de interconexión de sistemas abiertos. Modelo de arquitectura de redes desarrollado por ISO e ITU-T. El modelo consiste en siete capas, cada una de las cuales especifica funciones particulares de la red, como por ejemplo direccionamiento, control de flujo, control de errores, encapsulación y transferencia confiable de mensajes. La capa superior (capa de aplicación) es la más próxima al usuario; la capa inferior (capa física) es la más próxima a la tecnología de medios. La capa siguiente a la capa inferior está implementada en hardware y en software mientras que las cinco capas superiores están implementadas únicamente en software. El modelo de referencia OSI se utiliza mundialmente para enseñar y comprender la funcionalidad de una red. Es similar en ciertos aspectos a SNA. Véase capa de aplicación, capa de enlace de datos, capa de red, capa física, capa de presentación, capa de sesión, y capa de transporte.
<b>Módem</b>	Modulador-desmodulador. Dispositivo que convierte señales digitales y análogas. En el punto de origen, un módem convierte señales digitales a una forma apropiada para la transmisión por facilidades de comunicación análogas. En el punto de destino, las señales análogas se recuperan a su forma digital. Los módem permiten la transmisión de datos por líneas telefónicas de grado voz.
<b>Multicast</b>	Paquetes únicos copiados por la red y enviados a un subconjunto específico de direcciones de red. Estas direcciones están especificadas en el campo de dirección del destino.
<b>Multiplexación</b>	Técnica que permite la transmisión de varias señales lógicas simultáneamente a lo largo de un único canal físico.
<b>Multiplexor</b>	Dispositivo que permite a varios usuarios compartir un solo circuito. Canaliza diferentes flujos de datos en un solo cauce. Al otro extremo del enlace de comunicaciones, otro multiplexor invierte el proceso repartiendo los flujos de datos en los cauces originales.
<b>NAT (Network Address Translation)</b>	Traducción de direcciones de red. Un estándar definido en la RFC 1631 que permite a una red de área local (LAN) utilizar un conjunto de direcciones IP internamente y un segundo conjunto de direcciones externamente. El dispositivo que hace NAT se sitúa en el punto de salida a Internet y realiza todas las traducciones de direcciones IP que sean necesarias.
<b>NetBEUI (NetBIOS)</b>	Protocolo No enrutable propietario de Microsoft que es útil para redes pequeñas en

<b>Extended User Interface)</b>	ambientes Windows.
<b>NetBIOS (Network Basic Input/Output System)</b>	Sistema de básico de entrada/salida de red. API utilizada por aplicaciones en una LAN IBM para solicitar servicios de procesos de red de menor nivel. Estos servicios podrían incluir inicio y terminación de sesiones, y transferencia de información.
<b>NIC (Network Interface Card)</b>	Es una tarjeta que provee capacidades de comunicación de red para un sistema de cómputo.
<b>Nodo</b>	Punto final de una conexión de red, o unión común a dos o más líneas en una red. Los nodos pueden ser procesadores, controladores, o estaciones de trabajo. Los nodos, que pueden variar según su capacidad de enrutamiento y otras capacidades funcionales, pueden estar interconectados por enlaces, y servir como puntos de control en la red. El término nodo se emplea a veces de modo genérico para indicar cualquier entidad que puede tener acceso a una red, y es utilizado a menudo en forma intercambiable con dispositivo.
<b>NRM (normal response mode)</b>	Modo de respuesta normal. Modo HDLC para uso en enlaces con una estación primaria y una o más estaciones secundarias. En este modo, las estaciones secundarias pueden transmitir solamente si ellas reciben primero un sondeo de la estación primaria.
<b>NRZ (Non Return to Zero)</b>	Código sin retorno a cero. Las señales NRZ mantienen niveles de tensión constantes, sin transiciones de señal (sin retorno a un nivel de tensión cero) durante un intervalo de bit.
<b>NRZI (Non Return to Zero Inverted)</b>	Código sin retorno a cero invertido. Las señales NRZI mantienen niveles de tensión constantes, sin transiciones de señal (sin retorno a un nivel de tensión cero), pero interpretan la presencia de datos al comenzar un intervalo de bit como una transición de señal, y la falta de datos como una falta de transición.
<b>Orientado a conexión</b>	Término utilizado para describir la transferencia de datos que requiere el establecimiento de un circuito virtual.
<b>OSI (Open System Interconnection)</b>	Interconexión de sistemas abiertos. Programa de estandarización internacional creado por ISO e ITU-T para desarrollar normas para networking de datos que faciliten la interoperabilidad entre equipos de diversos fabricantes.
<b>OSPF (Open Shortest Path First)</b>	Protocolo de enrutamiento de estado de enlace, utiliza algoritmos complejos para calcular el costo de una ruta.
<b>PAP</b>	Password Authentication Protocol o Protocolo de Autenticación de Contraseña. Esquema de Autenticación para los enlaces PPP. Se puede especificar una contraseña para ambos dispositivos en el enlace remoto. El fracaso en la autenticación producirá la desconexión antes de que se inicie la transmisión de los datos.
<b>Paquete</b>	Agrupamiento lógico de información que incluye un encabezado que contiene información de control y (usualmente) datos del usuario. Los paquetes se utilizan más frecuentemente para hacer referencia a las unidades de datos de las capas de red. Los términos datagrama, frame, mensaje, y segmento también se utilizan para describir agrupamientos de información lógica en diferentes capas del modelo de referencia OSI y en varios círculos de tecnología.
<b>Paquete</b>	Es el conjunto de bits generalmente de capa 3 y 4 en el que se transmiten encapsulados los datos enviados, además de campos propios usados para la transmisión correcta de la información.
<b>Patch panel</b>	Es el recolector central del Cableado Estructurado, a través de él se puede tener concentrado todo al cableado de un número limitado de interfaces de determinado tipo.
<b>PHP</b>	Es un lenguaje de programación que se ejecuta en el servidor y se integra muy bien con el HTML y las bases de datos MySQL.
<b>PPP</b>	Protocolo de capa 2 que sirve para realizar conexiones seriales punto a punto.
<b>PPP (Point-to-Point Protocol)</b>	Protocolo punto a punto. Un sucesor de SLIP, PPP brinda conexiones enrutador a enrutador y host a red sobre circuitos síncronos y asíncronos.
<b>Protocolo</b>	<ol style="list-style-type: none"> <li>1. Descripción formal de un conjunto de reglas y convenciones que gobiernan la forma en la que los dispositivos de una red intercambian información.</li> <li>2. Campo dentro de un datagrama IP que indica el protocolo de capa superior (Capa 4) que envía el datagrama.</li> </ol>
<b>Protocolo de enrutamiento</b>	Protocolo que lleva a cabo el enrutamiento mediante la implementación de un algoritmo de enrutamiento específico. Entre los ejemplos de protocolo de enrutamiento se incluyen IGRP, OSPF y RIP.
<b>Protocolo enrutado.</b>	Protocolo que puede ser enrutado por un enrutador. Un enrutador debe ser capaz de

	interpretar la internetwork l3gica segun lo que especifica dicho protocolo enrutado. AppleTalk, DECnet, e IP son ejemplos de protocolos enrutados
<b>Puerto</b>	<ol style="list-style-type: none"> <li>1. Interfaz en un dispositivo de red (tal como un enrutador).</li> <li>2. En la terminología IP, un proceso de capa superior que está recibiendo información de capas más bajas.</li> </ol>
<b>PVC (Permanent Virtual Circuit)</b>	Circuito virtual permanente. Circuito virtual que se establece permanentemente. Los PVCs ahorran ancho de banda asociada con el establecimiento y corte del circuito en situaciones donde ciertos circuitos virtuales deban existir en todo momento.
<b>QoS (Quality of Service)</b>	Calidad de servicio. Medida de rendimiento de un sistema de transmisión que refleja su calidad de transmisión y disponibilidad de servicio.
<b>RARP (Reverse Address Resolution Protocol)</b>	Protocolo usado para mapear una dirección IP a una dirección MAC en redes No-broadcast como Frame Relay.
<b>Red</b>	Conjunto de computadoras, impresoras, enrutadores, switches, y otros dispositivos, que pueden comunicarse entre sí por algún medio de transmisión.
<b>Redundancia</b>	En la red, es la duplicación de dispositivos, servicios, o conexiones que, en caso de fallo, puedan realizar las tareas de aquéllos que hubieran fallado. Véase también sistema redundante.
<b>Reserva de ancho de banda</b>	Proceso que consiste en asignar ancho de banda a los usuarios y aplicaciones a los que sirve una red. Comprende la asignación de prioridad a los diversos flujos de tráfico basándose en cuán críticos y sensibles a los retrasos sean. Esto optimiza el uso del ancho de banda disponible y si la red se congestiona se puede descartar el tráfico con menor prioridad. También llamada asignación de ancho de banda.
<b>RIP (Routing Information Protocol)</b>	Protocolo de enrutamiento de vector distancia de la pila TCP/IP, se basa en saltos para calcular el costo de una ruta. Es el más simple que existe, pero funciona bien en redes pequeñas.
<b>RMON (Remote Monitoring)</b>	Protocolo que sirve para realizar operaciones de monitoreo en dispositivos de red.
<b>RS-232</b>	Conocida interfaz de capa física. Actualmente conocida como EIA/TIA-232.
<b>RS-422</b>	Implementación eléctrica balanceada de EIA/TIA-449 para la transmisión de datos a alta velocidad. Actualmente conocida en forma conjunta con RS-423 como EIA-530.
<b>RS-423</b>	Implementación eléctrica no balanceada de EIA/TIA-449 para la compatibilidad con EIA/TIA-232. Actualmente conocida en forma conjunta con RS-422 como EIA-530.
<b>RS-449</b>	Conocida interfaz de capa física. Actualmente conocida como EIA/TIA-449.
<b>Ruta estática</b>	Ruta explícitamente configurada e ingresada en la tabla de enrutamiento. Las rutas estáticas tienen prioridad sobre las rutas elegidas por los protocolos de enrutamiento dinámico.
<b>SDLC (Synchronous Data Link Control)</b>	Control de enlace de datos síncrono. Protocolo de comunicaciones de la capa de enlace de datos SNA. SDLC es un protocolo serial full duplex orientado al bit que ha dado origen a numerosos protocolos similares, incluidos HDLC y LAPB
<b>Segmento</b>	<ol style="list-style-type: none"> <li>1. Sección de una red unida por bridges, enrutadores y switches.</li> <li>2. En una LAN que utiliza topología de bus, un segmento es un circuito eléctrico continuo que suele estar conectado a otros segmentos por medio de repetidores.</li> <li>3. Término empleado en la especificación TCP/IP para describir a una única unidad de información de la capa de transporte. Los términos datagrama, trama, mensaje, y paquete también se utilizan para describir los grupos de información lógica de las diversas capas del modelo de referencia OSI y de varios círculos de tecnología.</li> </ol>
<b>Servidor</b>	Nodo o programa de software que brinda servicios a los clientes.
<b>Servidor de acceso</b>	Procesador de comunicaciones que conecta dispositivos asíncronos con una LAN o WAN mediante una red y un software de emulación de terminal. Realiza tanto enrutamiento asíncrono como síncrono de los protocolos soportados.
<b>Servidor Web</b>	Es un equipo terminal que se encarga de proporcionar el servicio de páginas web.
<b>Sesión</b>	Conjunto relacionado de transacciones de comunicación entre dos o más dispositivos de red.
<b>Shareware</b>	Tipo de licencia de uso en la que el programador que creo la aplicación o código fuente permite que cualquiera la pueda usar generalmente con un periodo de prueba regulado por limitaciones de las capacidades del programa, un tiempo de vida o una cantidad de veces que se puede usar. Esto para evaluar el software y de ser del agrado del que lo usa, este deberá

	dar una pequeña retribución con la condición aún no modificar el código.
<b>Sistema operativo</b>	Es el software encargado de la interactuar entre el usuario y el kernel encargado de controlar el hardware.
<b>SLIP (Serial Line Internet Protocol)</b>	Protocolo SLIP. Protocolo estándar para las conexiones seriales punto a punto que utiliza una variación de TCP/IP. Precursor de PPP.
<b>Sniffer</b>	Es un programa que monitorea y analiza el tráfico dentro de una red y gracias a su uso se puede detectar problemas y embotellamiento. También se denomina sniffer al uso legal o ilegal de captura de paquetes de información transmitida a través de una red. Esa es la razón por la que este segundo significado está más popularizado en la red.
<b>Socket</b>	Es la combinación de un Puerto TCP o UDP y una dirección IP.
<b>STP (Shielded Twisted-Pair)</b>	Par trenzado blindado. Medio de cableado de dos pares utilizado en una serie de implementaciones de red. El cableado STP tiene una capa de aislamiento blindada para reducir la EMI.
<b>Subred</b>	<ol style="list-style-type: none"> <li>1. En redes IP, red que comparte una dirección de subred particular. Las subredes son redes segmentadas arbitrariamente por un administrador de red para brindar una estructura de enrutamiento multinivel, jerárquico, protegiendo a la subred de la complejidad del direccionamiento de las redes conectadas. Llamada a veces subnet.</li> <li>2. En las redes OSI, grupo de ES e IS bajo el control de un único dominio administrativo que utilizan un mismo protocolo de acceso a la red.</li> </ol>
<b>SVC (Switched Virtual Circuit)</b>	Circuito virtual conmutado. Circuito virtual que se establece dinámicamente a petición y que se interrumpe cuando se completa la transmisión. Los SVC se utilizan en situaciones en las que la transmisión de datos es esporádica.
<b>Switch</b>	Dispositivo que concentra y distribuye las tramas de una red de área local
<b>Tabla de enrutamiento</b>	Tabla almacenada en un enrutador o en otro dispositivo de red que deja un rastro de las rutas hacia destinos particulares de la red y, en algunos casos, las métricas asociadas a dichas rutas.
<b>TCP (Transmission Control Protocol)</b>	Protocolos de control de transmisión. Protocolo de la capa de transporte orientado a conexión que provee una confiable transmisión de datos full-duplex. TCP es parte de la pila TCP/IP.
<b>Telecomunicaciones</b>	Término que se refiere a las comunicaciones (en general, involucra sistemas informáticos) por la red telefónica.
<b>Telnet</b>	Comando utilizado para verificar el software de la capa de aplicación entre las estaciones de origen y de destino. Éste es el mecanismo de prueba más completo disponible.
<b>Terminal</b>	Dispositivo simple donde se pueden ingresar o recuperar datos de una red. En general, las terminales tienen un monitor y un teclado, pero no tienen procesador ni unidad de disco local.
<b>TFTP</b>	Trivial File Transfer Protocol o Protocolo Trivial de Transferencia de Archivos. En equipos que ejecutan software de red TCP/IP, se usa TFTP para enviar archivos rápidamente a través de la red con menos seguridad que la que ofrece FTP.
<b>Throughput</b>	Caudal de información que llega a, y posiblemente atraviesa, un punto particular en un sistema de red.
<b>Token Ring</b>	LAN token passing desarrollada y soportada por IBM. Token Ring corre a 4 ó 16 Mbps por una topología de anillo. Similar a IEEE 802.5.
<b>Topología</b>	Disposición física de nodos y medios de red dentro de una estructura de networking empresarial.
<b>Trama</b>	Agrupamiento lógico de información enviada como unidad de capa de enlace de datos a través de un medio de transmisión. A menudo se refiere al encabezado y a la información final, utilizadas para la sincronización y control de errores, que rodean los datos del usuario contenidos en la unidad. Los términos datagrama, mensaje, paquete y segmento también se usan para describir agrupamientos de información lógica en las diversas capas del modelo de referencia OSI y en varios círculos tecnológicos.
<b>Transceiver (transceptor)</b>	El dispositivo real que une la red y el nodo local. El término generalmente se refiere a cualquier conector, como un MAU que activamente convierte señales entre la red y el nodo local.
<b>Transmisión analógica</b>	Transmisión de señales por cables o por aire, en la cual se conduce información a través de

	una variación de cierta combinación de amplitud, frecuencia y fase de señal.
<b>Transmisión asíncrona</b>	Término que describe las señales digitales que se transmiten sin una sincronización precisa. Esas señales en general tienen distintas frecuencias y relaciones de fase. Las transmisiones asíncronas, en general, encapsulan caracteres individuales en bits de control (llamados bits de inicio y parada) que designan el comienzo y el fin de cada carácter.
<b>Transmisión síncrona</b>	Término que describe las señales digitales que se transmiten con una precisa sincronización. Dichas señales tienen la misma frecuencia, con caracteres individuales encapsulados en bits de control (llamados bits de arranque y bits de parada) que designan el inicio y el fin de cada carácter.
<b>Trap</b>	Mensaje enviado por un agente SNMP a un NMS, consola, o terminal, para indicar la ocurrencia de un evento significativo, como una condición definida específicamente, o un umbral que ha sido alcanzado.
<b>UDP (User Datagram Protocol)</b>	Protocolo de datagrama de usuario. Protocolo sin conexión de capa de transporte en la pila TCP/IP. UDP es un protocolo simple que intercambia datagramas sin confirmación o garantía de entrega y que requiere que el procesamiento de errores y las retransmisiones sean manejados por otros protocolos. UDP se define en la RFC 768.
<b>URL (Uniform Resource Locator)</b>	Localizador Universal de Recurso. Es el nombre que reciben las diversas cosas e información que se pueden encontrar en la Red: páginas Web (http), archivos (ftp) o grupos de noticias (mail). Al escribir el nombre completo de un recurso en este formato, se accede a él, normalmente desde un programa navegador o software específico
<b>UTP (unshielded twisted-pair)</b>	Par trenzado sin blindaje. Medio de cables de cuatro pares utilizado en varias redes. UTP no requiere de un espacio fijo entre conexiones que sí es necesario con las conexiones de tipo coaxial. Hay cinco tipos de cableados UTP de uso común: cableado de categoría 1, cableado de categoría 2, cableado de categoría 3, cableado de categoría 4, y cableado de categoría 5.
<b>V.24</b>	Estándar ITU-T para una interfaz de capa física entre DTE y DCE. V.24 es esencialmente lo mismo que la norma EIA/TIA-232.
<b>V.32</b>	Protocolo de línea en serie del estándar ITU-T para las transmisiones bidireccionales de datos a velocidades de 4,8 ó 9,6 Kbps.
<b>V.32bis</b>	Estándar ITU-T que extiende la V.32 a velocidades de hasta 14,4 Kbps.
<b>V.34</b>	Estándar ITU-T que especifica un protocolo de línea en serie. V.34 ofrece mejoras respecto del estándar V.32, entre las que se incluyen mayores velocidades de transmisión (28,8 Kbps) y mejor compresión de datos.
<b>V.35</b>	Estándar ITU-T que describe un protocolo de capa física síncrono utilizado para las comunicaciones entre un dispositivo de acceso a la red y una red de paquetes. V.35 se utiliza más comúnmente en Estados Unidos y Europa, y está recomendado para velocidades de hasta 48 Kbps.
<b>VLSM (Máscara de Subred de Longitud Variable)</b>	Método que permite la utilización de máscaras de subred de longitud variable.
<b>WAN (wide-area network)</b>	Red de área amplia. Red de comunicación de datos que sirve a usuarios ubicados a través de una amplia zona geográfica y a menudo utiliza dispositivos de transmisión suministrados por portadoras comunes. Frame Relay, SMDS y X.25 son ejemplos de WAN.
<b>WWW (World Wide Web)</b>	Es una red mundial de páginas de información hipertexto, por la que se puede circular mediante un navegador Web.
<b>X.25</b>	Estándar ITU-T que define cómo se mantienen las conexiones entre DTE y DCE para el acceso a terminales remotas y las comunicaciones entre computadores en PDNs. X.25 especifica LAPB, un protocolo de capa de enlace de datos, y PLP, un protocolo de capa de red. Frame Relay ha reemplazado en cierta medida a X.25.
<b>XML (Extensible Markup Language)</b>	Lenguaje de Marcas Ampliable, es una forma flexible de crear formatos de información y compartir tanto el formato como los datos en la World Wide Web, intranets y otras redes. El XML es actualmente una recomendación formal del World Wide Web Consortium como una forma de hacer de la Red una herramienta más versátil. El XML es similar al lenguaje de las páginas web actuales, el HTML, ya que ambos contienen símbolos de marcas para describir los contenidos de una página o archivo.

---

## Bibliografía y fuentes electrónicas de consulta y referencia.

- **Computer Networks**  
Uyless Black  
Pretince Hall PTR  
Capítulo 1.
- **Top-Down Network Design.**  
Priscilla Oppenheimer.  
Mcmillan Technical Publishing & Cisco Press. 1999.  
Capítulos 1, 2, 3, 4, 6, 7, 8, 9 y 10.
- **Local and Metropolitan Area Networks.**  
William Stallings.  
Pentice Hall. 1997.  
Capítulos 1, 2 y 3.
- **Building Cisco Remote Access Networks.**  
Catherine Paquet.  
Cisco Press. 1999.  
Capítulos 4 y 5.
- **TCP/IP Running a Successful Network.**  
K. Washburn. J.T Evans  
Capítulos 4 y 5
- **Cisco IOS essentials.**  
Jhon Albriton.  
Mc Graw Hill.  
Capítulos 9, 11 y 12.
- **Protecting your web site with firewalls.**  
Marcus Goncalves.  
Prentice Hall.  
Capítulo 10.
- **CCNA study guide.**  
Osborne 1998.  
Capítulos 9, 10, 11, 12 y 13.
- **IP Routing Primer.**  
Robert Wright.  
Mc Graw Hill.  
Capítulos 11 y 14.

## Referencias electrónicas.

### Capítulo 1

- [http://www.dsic.upv.es/~mrebollo/ofimatica/download/redes\\_internet.pdf](http://www.dsic.upv.es/~mrebollo/ofimatica/download/redes_internet.pdf)

### Capítulo 2



- 
- <http://www.ots.utexas.edu/ethernet/>
  - [http://www.cisco.com/univercd/cc/td/doc/cisintwk/ito\\_doc/tokenrng.htm](http://www.cisco.com/univercd/cc/td/doc/cisintwk/ito_doc/tokenrng.htm)
  - <http://www.cisco.com/univercd/cc/td/doc/product/lan/cat3900/3900ug4/cables.htm>
  - <http://support.intel.com/support/tokenexpress/6302.htm>
  - [http://www.cisco.com/univercd/cc/td/doc/cisintwk/ito\\_doc/fddi.htm](http://www.cisco.com/univercd/cc/td/doc/cisintwk/ito_doc/fddi.htm)

#### Capítulo 3.

- <http://www.mouse.demon.nl/ckp/lanwan/ieee8022.htm>
- <http://www.optimized.com/COMPENDI/L1-L.LC.htm>
- [http://www.cisco.com/univercd/cc/td/doc/cisintwk/ito\\_doc/introlan.htm](http://www.cisco.com/univercd/cc/td/doc/cisintwk/ito_doc/introlan.htm)
- <http://www.optimized.com/COMPENDI/>
- [http://www.cisco.com/univercd/cc/td/doc/cisintwk/ito\\_doc/ethernet.htm](http://www.cisco.com/univercd/cc/td/doc/cisintwk/ito_doc/ethernet.htm)
- [http://www.cisco.com/univercd/cc/td/doc/cisintwk/ito\\_doc/ethernet.htm](http://www.cisco.com/univercd/cc/td/doc/cisintwk/ito_doc/ethernet.htm)
- <http://www.optimized.com/COMPENDI/L1-FastE.htm>

#### Capítulo 4

- [http://www.cisco.com/univercd/cc/td/doc/cisintwk/ito\\_doc/sdlcetc.htm](http://www.cisco.com/univercd/cc/td/doc/cisintwk/ito_doc/sdlcetc.htm)
- <http://www.wmpenn.edu/pennweb/academic/artstech/compsci/networks/sdlc/sdlc.html>
- <http://pelt.cis.yale.edu/pelt/COMM/SNA.11TM>

#### Capítulo 5

- <http://www.cis.ohio-state.edu/hypertext/information/rfc.html>
- <http://dmoz.org/World/Español/Computadoras/Internet/Protocolos/>
- <http://www.cis.ohio-state.edu/hypertext/information/rfc.html>
- <http://dmoz.org/World/Español/Computadoras/Internet/Protocolos/>
- <http://www.saulo.net>

#### Capítulo 9.

- <http://www.redaccionvirtual.com/redaccion/glosario/default.asp>
- [http://www.rad.com/products/prod\\_fam.htm](http://www.rad.com/products/prod_fam.htm)
- <http://www.cisco.com/univercd/cc/td/doc/product/lan/cat2600/c26userg/token.htm>

#### Capítulo 10.

- <http://www.dtd.unam.mx/Normatividad/redunam.html>
- <http://mssimplex.com/proxis&Firewalls.htm>
- <http://www.cisco.com/univercd/cc/td/doc/product/software/ios113cd/cs/csprtn1/csrp.htm>
- [http://www.fatkid.com/html/101\\_reverse\\_telnet.html](http://www.fatkid.com/html/101_reverse_telnet.html)

#### Capítulo 13.

- [http://www.cisco.com/public/products\\_tech.shtml](http://www.cisco.com/public/products_tech.shtml)
- <http://www.redaccionvirtual.com/redaccion/glosario/>
- <http://www.protocols.com/pbook/tcpip.htm>

#### RFCs consultadas.

- RFC - 2663. NAT.
- RFC - 1631. NAT.
- RFC - 1918. Asignación de direcciones IP para redes privadas.
- RFC - 1583. OSPF v.2.
- RFC - 1793. Extensiones de OSPF que soportan demandas de Circuitos.
- RFC - 1586. Guía de estudio para usar OSPF sobre Redes Frame Relay.

- 
- RFC - 1584. Extensiones de Multienvío o Multidifusión para OSPF.
  - RFC - 1403. Interacción entre OSPF y BGP.
  - RFC - 116. Las direcciones usadas en Internet.
  - RFC - 791. El protocolo IP.

**Manuales y referencias electrónicas on-line en formato pdf de CCO ([www.cisco.com](http://www.cisco.com).)**

- PPP.
- RIP.
- IGRP.
- EIGRP.
- OSPF.
- Frame Relay