ESCUELA POLITECNICA NACIONAL

FACULTAD DE INGENIERIA ELECTRICA

ESTUDIO Y DISEÑO DE UNA RED ESTRUCTURADA DE DATOS LOCAL

TESIS PREVIA A LA OBTENCION DEL TITULO DE INGENIERIO EN LA ESPECIALIDAD DE ELECTRONICA Y TELECOMUNICACIONES

RODRIGO VINICIO CHAVEZ RIVAS

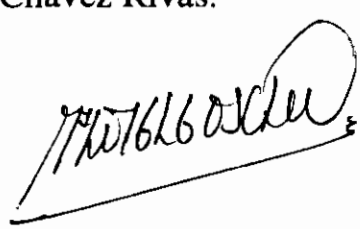
QUITO, OCTUBRE DE 1997

AGRADECIMIENTO

Agradezco a Dios por haberme dado salud y vida, a mis padres y hermanos por su incansable apoyo durante los años de mi carrera y a todas las personas e instituciones que hicieron posible la culminación de este trabajo.

Mi agradecimiento especial al Ing. Pablo Hidalgo por su inmejorable dirección y apoyo en el desarrollo de esta tesis.

Certifico que la presente tesis ha sido elaborada en su totalidad por el señor Rodrigo Vinicio Chávez Rivas.



Ing. Pablo Hidalgo Lascano
DIRECTOR DE TESIS

PREFACIO

Las tecnologías de comunicación de datos están en constante evolución y expansión. El crecimiento en demanda de conectividad de redes en el ámbito LAN y WAN requiere de una rápida y completa adaptación de esta tecnología tanto en la fase de desarrollo como de implementación. Desgraciadamente, los recursos de información sobre tecnologías de conectividad y redes estructuradas de datos, no siempre están actualizados el momento de su impresión. Esta tesis no es la excepción, sin embargo, se ha tratado de mantener información lo más actualizada posible, organizándola de forma que siga una secuencia lógica para su fácil entendimiento.

OBJETIVO

Se espera que esta tesis, en conjunto con otros documentos y herramientas (exploradores de Internet por ejemplo), pueda servir como una guía útil a quienes estén interesados en conocer sobre redes estructuradas de datos y tecnologías de conectividad.

ENFOQUE

Esta tesis se ha escrito para quienes están interesados en conocer de una manera introductoria pero organizada, sobre redes estructuradas de datos de área local, y tecnologías de conectividad para redes de área local.

ORGANIZACIÓN

Esta tesis se ha divido en seis capítulos. Los primeros tres capítulos están relacionados con material introductorio a las redes estructuradas de datos y tecnologías de conectividad para redes de área local. En los capítulos cuarto y quinto, se realiza el diseño y análisis (técnico y económico) de una red estructurada de datos local para una entidad hipotética. En el sexto capítulo se presentan las conclusiones y recomendaciones para el tema en estudio.

- Capítulo 1, "Introducción a un sistema de red estructurado de datos", presenta conceptos básicos para el entendimiento de la infraestructura de transporte, subsistema de conectividad, su ubicación dentro de un sistema de red estructurado de datos, y su relación con el Modelo OSI. Se realiza una explicación clasificatoria del Modelo de Referencia OSI, con el objeto de facilitar el entendimiento de los siguientes capítulos.
- Capítulo 2, "Infraestructura de transporte de una red estructurada de datos, evaluación y administración", presenta una visión general de lo que es una infraestructura de transporte estructurada, su evolución, y su sistema actual en vigencia: cableado estructurado.
- Capítulo 3, "Subsistema de conectividad de una red estructurada de datos, evaluación y administración", describe el subsistema de conectividad enfocado en dos partes: dispositivos de conectividad y protocolos de comunicación para redes de área local.
- Capítulo 4, "Análisis y diseño de un subsistema de conectividad integrada sobre un sistema de cableado estructurado de una red hipotética de datos", describe el análisis y

diseño del subsistema de conectividad de una entidad hipotética, considerando que existe un sistema de cableado estructurado implementado.

- Capítulo 5, "Análisis de inversión", describe el análisis de costos que debe realizarse para una buena selección de varias alternativas solución planteadas en el capítulo 4.
- Capítulo 6, "Conclusiones y recomendaciones".
- Bibliografía
- Anexos

CAPITULO I

CAPITULO II

CAPITULO III

CAPITULO IV

CAPITULO V

CAPITULO VI

Capítulo I

Introducción a un sistema de red estructurado de datos local

I. INTRODUCCION A UNA RED ESTRUCTURADA DE DATOS LOCAL

1.1 GENERALIDADES

La evolución tecnológica ha sido marcada durante toda la historia fundamentalmente por la imperiosa necesidad de producir más con menos recursos. Los sistemas de comunicación de datos, no han sido la excepción.

No obstante esta evolución tecnológica, es tranquilizante conocer que mucho de lo que se ha desarrollado, y en algunas ocasiones puede sonar como novedoso, está fundamentado en bases utilizadas desde siempre, y de las cuales se tiene pleno conocimiento. Nos corresponde, en el caso de los sistemas de comunicación de datos, hacer referencia a la forma en que se han manejado las redes de datos tradicionalmente.

Desde que se iniciaron las redes de datos con sistemas centralizados, a lo largo de los sistemas distribuidos y sistemas colaborativos, las redes han mantenido una estructura fundamentada en cuatro partes básicas:

1. Servidores y equipos de aplicaciones
2. Infraestructura de transporte
3. Subsistema de conectividad
4. Dispositivos de escritorio

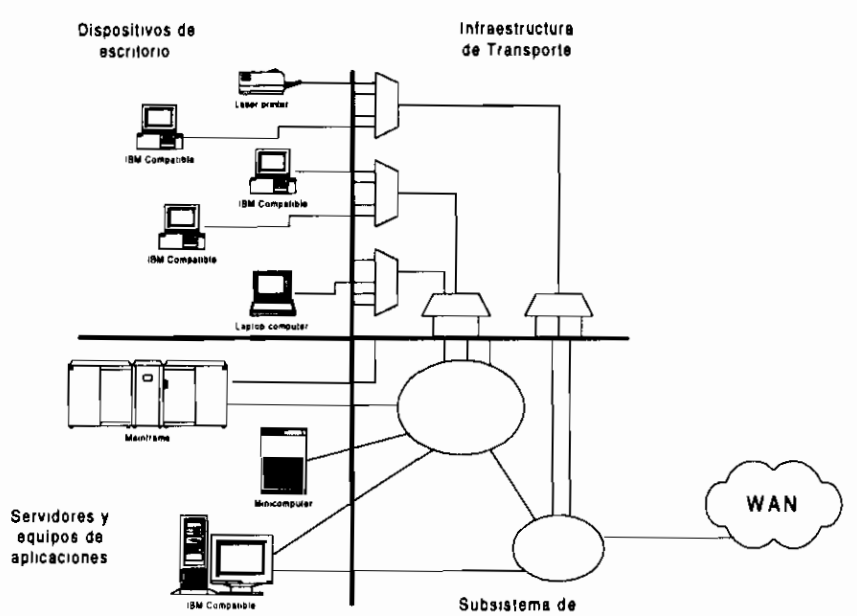


***Figura 1.1* Subsistemas de una red estructurada de datos**

Estos cuatro subsistemas se han mantenido independientes del tipo de red en cuanto a tamaño se refiere, sean redes LAN, MAN o WAN. En lo posterior, nos

referiremos a las 4 partes básicas como subsistemas, dentro de lo que sería el sistema red de datos.

Para aclarar lo que comprenden cada uno de los subsistemas señalados, es prudente hacer mención de los requerimientos fundamentales de una red. Estos son:

- Dos o más entes que tengan algo que compartir.
- Método o camino que les permita ponerse en contacto.
- Una serie de normas que permitan a esos entes comunicarse.

De esta forma, los servidores o equipos de aplicaciones y los dispositivos de escritorio, son los subsistemas que podrían considerarse como los entes que tienen algo para compartir y son los servicios de red. Dentro de los servicios de red, pueden enumerarse los siguientes:

- Servicios de archivos
- Servicios de impresión
- Servicios de mensajes
- Servicios de aplicaciones
- Servicios de base de datos
- Servicios especializados

Si se hace una analogía con dos personas que quieren comunicarse telefónicamente, aquellas personas tendrán algún interés para conversar, de lo contrario será muy poco productivo que los dos entes lleguen a hablar. Además requerirán de un interfaz que les permita comunicarse a través del medio de transmisión, en el caso de redes de datos las interfaces de red, y en el caso de la analogía, el teléfono.

El subsistema de infraestructura de transporte puede considerarse como el medio o camino por el cual viajarían los datos del un ente al otro. Esto significa que la infraestructura de transporte garantiza el medio por el cual los entes podrían ponerse en contacto, mas no la conexión misma. Siguiendo con la analogía, en el caso más sencillo de comunicación por teléfono, no se requeriría conmutación, es decir, simplemente se levantarían los auriculares y podría establecerse la conexión entre dos personas. En el caso de datos podría darse el mismo evento, sin embargo la necesidad de comunicación no es sólo entre dos personas, por tal motivo existen lo que se conocen como centrales telefónicas de conmutación. De la misma forma, para las redes de datos son necesarios dispositivos que permitan el establecimiento de la conexión entre dos o más entes. A este conjunto de dispositivos que se encargan de "decidir" los caminos por los cuales se establecerá la conexión entre los entes, se lo conoce como subsistema de conectividad.

Continuando con la analogía, una vez garantizado el camino físico y establecida la conexión, las personas podrán conversar a través de sus aparatos telefónicos, siempre y cuando hablen el mismo idioma. En las redes de datos, el conjunto de normas que permiten la comunicación se los conoce como protocolos de comunicación.

Una vez que se tienen todos los elementos que se han mencionado, aparentemente el sistema de red de datos es completo. Esto es cierto si se considera que la red será integrada con dispositivos de un único proveedor, sin embargo se sabe que los proveedores de dispositivos de redes son muchos, y no necesariamente tendrían que utilizar los mismos interfaces y protocolos. Por esta razón, en 1977, la *International Standard Organization (ISO)*, creó un subcomité para desarrollar estándares de comunicación de datos para la interfuncionabilidad de multiproveedores. Fruto de este trabajo es el Modelo de Referencia OSI *(Open System Interconnection)*. El modelo de referencia sirve como guía funcional para la división de las tareas de comunicación, estableciendo de esta manera parámetros que permitan a los proveedores, desarrollar productos que sean abiertos al sistema, es decir compatibles con los de otros proveedores, sin que antes tengan que ponerse de acuerdo. Tradicionalmente se ha venido utilizando este modelo, pues ha sido el más ampliamente aceptado.

Hasta el momento, se ha enfocado el esquema global de una red de datos como sistema, con el objetivo de ubicar a cada uno de los subtemas que serán tratados con mayor profundidad en los capítulos posteriores del presente trabajo. Dado que el tema hace referencia a una red estructurada de datos local, nos centraremos en lo posterior al estudio de sistemas estructurados para redes locales, y dentro de esto a los subsistemas referentes a infraestructura de transporte y subsistema de conectividad. No se incluye el estudio de los subsistemas referentes a servidores y equipos de aplicaciones ni a los dispositivos de escritorio o usuario final debido su extensión, dejando la posibilidad de un estudio posterior de los mismos.

Se incluirá además en este trabajo, una revisión del modelo de referencia OSI, describiendo detalladamente los tres primeros niveles, y se realizará una descripción resumida de los cuatro niveles superiores.

1.2 MODELO DE REFERENCIA OSI

El modelo de referencia OSI, nació de la necesidad de que los protocolos de los diferentes fabricantes de dispositivos de redes de datos logren comunicarse entre sí más fácilmente. El modelo consiste de siete capas cada una de las cuales especifica funciones particulares de red tales como direccionamiento, control de flujo, control de errores, encapsulamiento, transferencia confiable de mensajes. La capa más alta (la capa de aplicación) es la más cercana al usuario; la capa más baja (la capa física) es la más cercana a la tecnología del medio de transmisión.

En la mayoría de los sistemas, el conseguir la funcionalidad de un todo es relativamente fácil si una persona o un mismo grupo de ellas, son las que desarrollan el producto totalmente. En la práctica, se sabe que en la mayoría de los casos, varios proyectos se llevan a cabo paralelamente por diferentes empresas o grupos humanos, lo que implica que en un momento determinado se tendrá que decidir entre las ofertas de varios fabricantes de un mismo producto. Hoy en día esta tarea se orienta a la búsqueda de componentes que sean lo más compatibles posibles, es decir, la búsqueda está

orientada a lo que son los sistemas abiertos. El establecer un modelo nos ayuda a cumplir con este propósito.

1.2.1 DIVISION EN CAPAS DE LOS MODELOS DE REFERENCIA

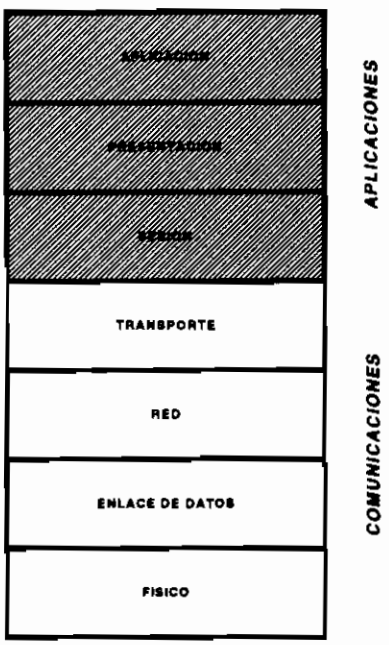


***Figura I.2** Capas del modelo de referencia OSI*

En la mayoría de ambientes de comunicaciones, existe una separación entre lo que son las funciones de comunicaciones y las funciones de los procesos de aplicación. Esta separación de las funciones de conectividad han sido definidas como niveles o capas. Para el modelo de referencia OSI siete capas numeradas indican las diferentes funciones. Dentro del modelo TCP/IP por ejemplo, se distinguen cinco capas funcionales. Sin considerar el número de capas, las razones para esta división de las funciones de red incluyen las siguientes:

- Dividir los aspectos interrelacionados de las operaciones de conectividad en elementos menos complejos.
- Definir interfaces estándar para compatibilidad *plug-and-play* e integración multiproveedor.
- Permitir a los ingenieros diseñar y desarrollar sobre funciones modulares.
- Proveer simetría en las diferentes funciones modulares de conectividad para que ellas interoperen.
- Prevenir cambios en una área de impacto para otras áreas, así que cada área pueda desenvolverse rápidamente.
- Dividir la complejidad de la conectividad.

1.2.2 CAPAS DEL MODELO DE REFERENCIA OSI

El modelo de referencia OSI hace referencia a las siguientes siete capas:

1. Capa física
2. Capa enlace de datos
3. Capa red
4. Capa transporte
5. Capa sesión
6. Capa presentación
7. Capa aplicación

Los capas o niveles se numeran comenzando por la capa física como nivel 1; cada nivel representa un grupo de tareas específicas. Se debe notar que algunas implementaciones podrían no asociarse con todos los niveles, debido a que las capas se definieron de acuerdo a las funciones que sus creadores les asignaron, y en muchos de los casos las implementaciones se desarrollaron antes de que el modelo existiera, como por ejemplo la implementación de protocolos TCP/IP.

1.2.3 INTERACCION DE LOS NIVELES

La función que realizan las implementaciones según el modelo, es proporcionar servicios a la implementación correspondiente de nivel superior, es decir, la implementación asociada al nivel N utiliza los servicios de la implementación asociada al nivel N-1, y brinda servicios a la implementación asociada al nivel N+1. Para que los mensajes de un computador lleguen a otro, el mensaje deberá viajar desde el nivel más alto de su propio *stack* de protocolos[1] hasta su nivel más bajo, donde en calidad de bits llegará hasta el nivel más bajo del *stack* del otro computador, ascendiendo en este último hasta el nivel más alto.

Las comunicaciones *peer-to-peer* (entre dos equipos) a través de dos *stacks* diferentes, se consigue mediante el proceso de encapsulamiento. Cada capa utiliza su propio protocolo de capa para comunicarse con su capa par en el otro sistema. Cada protocolo de capa intercambia información llamada unidades de datos del protocolo (PDU) ó unidades de datos de servicio entre capas pares. Comúnmente se utilizan los siguientes nombres:

- Nivel físico - bits
- Nivel enlace de datos - tramas
- Nivel red - paquetes
- Nivel aplicaciones - mensajes

[1] El *stack* o pila de protocolos es un conjunto jerárquico de protocolos que trabajan conjuntamente. Cada uno de ellos da servicio al protocolo superior, y recoge un servicio del protocolo inferior. De esta forma cada protocolo puede ser asociado a un nivel OSI.

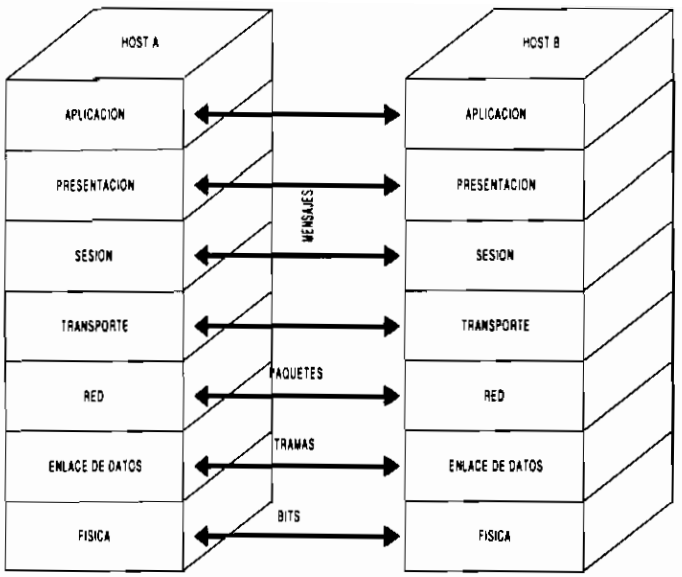


***Figura 1.3** Unidades de datos de protocolos (PDU) por capas*

Cada capa depende de la función de servicio que le sigue. Para proveer este servicio, las capas más bajas utilizan el encapsulamiento para poner el PDU desde la capa más alta dentro de su campo de datos; entonces aquella puede añadir cualquier cabecera y cola *(trailer)* a la capa que usará para realizar su función.

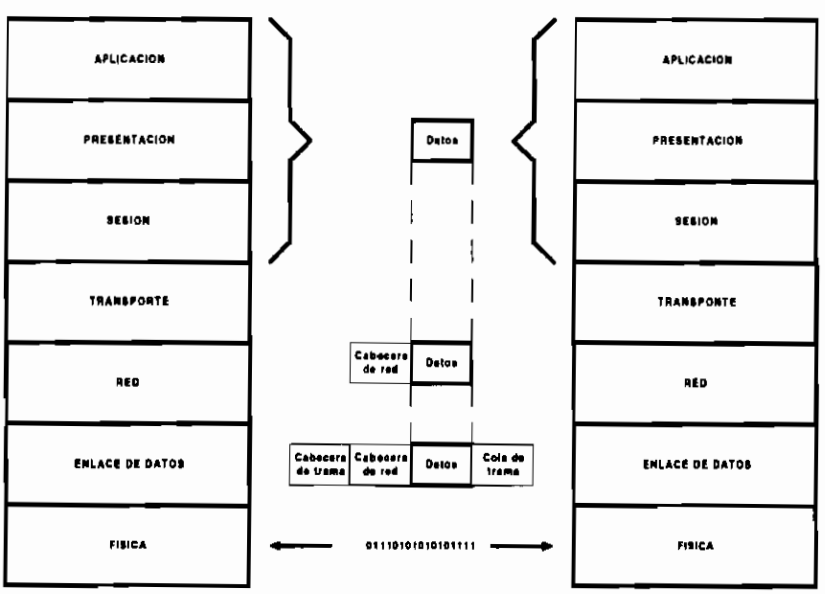


***Figura 1.4** Utilización de cabeceras en el proceso de encapsulamiento de datos*

Por ejemplo, la capa red provee un servicio a la capa transporte, y la capa transporte presenta "datos" a las capas superiores.

La capa red tiene la tarea de mover datos a través de la red. Aquella cumple esta tarea por encapsulamiento de los datos dentro de una cabecera. Esta cabecera contiene

información requerida para completar la transferencia, tales como direcciones lógicas de fuente y destino.

La capa enlace de datos provee un servicio a la capa red. Aquella encapsula la información de la capa de red en una trama. La cabecera de la trama contiene información requerida para completar las funciones de enlace de datos. Por ejemplo, la cabecera de trama contiene las direcciones físicas.

Finalmente, la capa física provee un servicio a la capa enlace de datos. Este servicio incluye codificación de los datos enlazados a la trama dentro de un patrón de 1s y 0s para la transmisión sobre el medio.

1.2.4 UTILIZACION PRACTICA DE LOS MODELOS

El modelo de referencia OSI no es tangible. La comunicación de la red requiere que los protocolos específicos se conviertan en procesos tangibles.

Aunque dos protocolos puedan estar asociados a los mismos niveles del modelo OSI, tal vez no funcionen juntos. Posiblemente el mejor uso del modelo es categorizar las tecnologías de conectividad y sus implementaciones de protocolos. Es decir, el modelo de referencia es útil para asignar categorías a los distintos protocolos dependiendo de sus funciones. Servirá entonces, como armazón conceptual para agrupar protocolos y productos similares.

1.2.5 NIVELES DEL MODELO DE REFERENCIA OSI RELACIONADOS CON EQUIPO DE CONECTIVIDAD

Debido a la orientación del presente trabajo, las capas a las cuales se les brindará mayor atención son:

- Capa física
- Capa enlace de datos
- Capa red

El resto de niveles se hará referencia con menor detenimiento. El formato[2] que se establecerá comprenderá para cada nivel una serie de temas a tratarse y dentro de cada tema las técnicas utilizadas en ese nivel.

[2] Este formato se ha tomado del Manual del alumno del curso de Tecnologías de Conectividad de Novell. En vista de que la referencia bibliográfica encontrada es completa y didáctica, el esquema se lo sigue de forma muy similar, complementando determinados aspectos con información de otras fuentes bibliográficas.

1.2.5.1 El nivel físico OSI

Las unidades de datos en este nivel son conocidas como bits. Las implementaciones del protocolo del nivel físico OSI coordinan las normas para la transmisión de bits. Este nivel define:

1. Estructuras físicas de la red.
2. Especificaciones mecánicas y eléctricas para la utilización del medio de transmisión.
3. Normas de codificación y sincronización para la transmisión de bits.

El nivel físico no incluye una descripción del medio; sin embargo, las implementaciones de los protocolos del nivel físico son específicas del medio de transmisión.

A. *Hardware* de conectividad de red asociado con el nivel físico OSI

1. Concentradores y repetidores:

   Función: Los concentradores se encargan de distribuir las señales eléctricas. Los repetidores regeneran las señales eléctricas de datos. Debe notarse que dentro de los concentradores se pueden encontrar concentradores pasivos y activos. Los primeros sólo distribuyen la señal, pero los activos además se encargan de regenerar la señal, es decir son concentradores (hubs) y además repetidores.

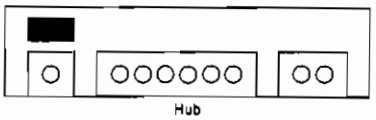


***Figura 1.5* Hub o concentrador de acceso compartido**

2. Conectores del medio de transmisión:

   Función: Proporcionar la interfaz mecánico para interconectar los dispositivos con el medio de transmisión.

3. Modems y Codecs

   Función: Realizar conversiones analógicas y digitales.

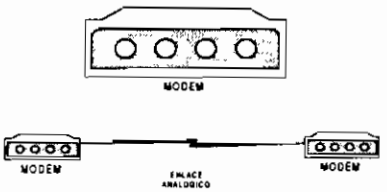


***Figura 1.6* Enlace entre modems**

4. CSU/DSU (Unidad de servicio de canal/Unidad de servicio digital):

Función: Son dispositivos que preparan las señales de impulsos eléctricos para su transmisión sobre medios de transmisión WAN.

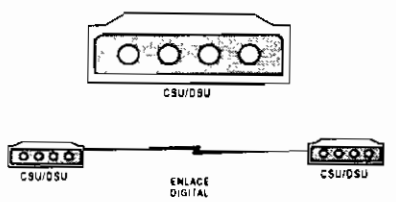


Figura 1.7 Enlace entre CSU/DSU

B. Temas y técnicas del nivel físico OSI

Nivel OSI	Tema	Técnicas
Físico	Tipos de conexión	Punto a punto Multipunto
	Topología física	Bus Anillo Radial Combinada Celular
	Señalización digital	
	Señalización analógica	
	Sincronización de bits	Asíncrono Síncrono
	Uso del ancho de banda	Banda ancha Banda Base
	Multiplexión	División de frecuencia (FDM) División de tiempo (TDM) División estadística del tiempo (STDM)

Tabla 1.1 Temas y técnicas del nivel físico OSI

B.1 Tipos de conexión

Definen la forma en que se establece la conexión física de los dispositivos a un segmento de red. El principal factor a considerar dependiendo del tipo de conexión es el ancho de banda[3] que le corresponde a cada dispositivo.

[3] Una señal digital en teoría necesita un ancho de banda infinito para transmitirse. En la práctica requiere el 90% de la energía del pulso. Dado un ancho de banda B, y M el número de símbolos posibles, el número máximo de bits por segundo que pueden transmitirse es: Rmáx = $2B\log_2 M$ [bps]

a. Conexión punto a punto

Es el tipo de conexión en el que dos ETDs (Equipo Terminal de Datos) tienen un enlace directo. Debido a que sólo dos dispositivos comparten la conexión punto a punto, cada estación tiene garantizado un ancho de banda específico.
Se forman redes locales y de amplia cobertura del tipo "almacenar y enviar" (*store and forward*).
Soportan varias topologías.

b. Conexión multipunto

Es el tipo de conexión en el que tres o más ETDs comparten un mismo enlace. Por el tipo de conexión, el ancho de banda disponible para cada dispositivo es dividido para el número de dispositivos que comparten el medio.
Economizan equipos de comunicaciones, pero la administración del canal y control del diálogo son más complejos.
Los tiempos de respuesta por lo general serán mayores con relación a la conexión punto a punto.
Es utilizada en la mayoría de redes locales.

B.2 Topología física

La topología física establece la forma en que las estaciones estarán interconectadas. Busca cumplir con tres objetivos:

1. Máximar la fiabilidad para garantizar la recepción correcta de todo el tráfico.
2. Utilizar el camino de la manera más económica posible.
3. Proporcionar al usuario un tiempo de respuesta óptimo y un caudal eficaz máximo.

Al escoger una topología física, deberán considerarse las siguientes características:

- Facilidad de instalación
- Facilidad de reconfiguración
- Facilidad de localización de averías
- Mínimo número de unidades afectadas en caso de falla del medio

Tipos de topología física

Se debe notar que todas las topologías tienen limitaciones de distancia y de número de dispositivos conectados, para lo cual se han diseñado varios protocolos que abordan estas limitaciones y hacen más sencillas las instalaciones.

a. Topología de bus

Suele utilizar un único cable denominado "auxiliar o *backbone*" al cual se conectan todos los dispositivos. Podría decirse que está formado por enlaces punto a punto en serie. Los cables cortos que unen el backbone con los ETDs se los denomina cables de tendido. A los puntos en donde se intersecan los cables de tendido con el *backbone* se los denomina derivaciones del cable. Físicamente las derivaciones del cable suelen ser conectores en T. El *backbone* deberá tener terminaciones en ambos extremos para suprimir la señal del cable e impedir el rebote de la señal por el mismo.

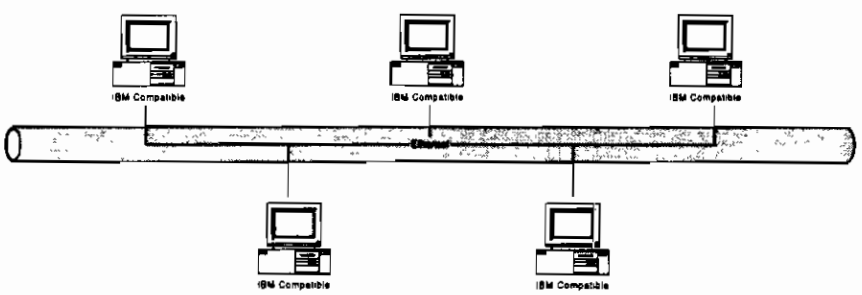


Figura 1.8 Topología física en bus

La mayoría de las topologías en bus permiten a los datos viajar bidireccionalmente.

Ventajas	Inconvenientes
Fácil de instalar utilizando estándares establecidos.	Difícil de reconfigurar, especialmente si la configuración ha llegado a su límite de permisibilidad.
Requiere menos infraestructura de transporte que otras topologías.	La localización de averías es dificultosa.
	En caso de falla en el medio, todas las unidades se ven afectadas.

Tabla 1.2 Ventajas e inconvenientes de la topología física en bus

b. Topología en anillo

Es una topología circular o de bucle cerrado de enlaces punto a punto. Cada ETD se conecta al anillo directo o indirectamente mediante un dispositivo de interfaz y un cable de tendido.

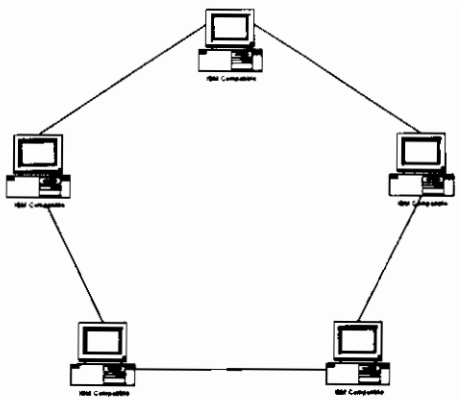


Figura 1.9 Topología física en anillo

Por lo general la topología en anillo transmite los datos en una sola dirección. Debido a que la señal se regenera en cada ETD, la degradación de la señal es mínima.
Por efectos de tolerancia a fallos, las topologías en anillo se suelen configurar con doble bucle. Los dobles anillos son físicamente distintos, transmitiendo cada uno de ellos en una dirección distinta. Las transmisiones en direcciones diferentes se pueden utilizar para rodear un único fallo del cable.

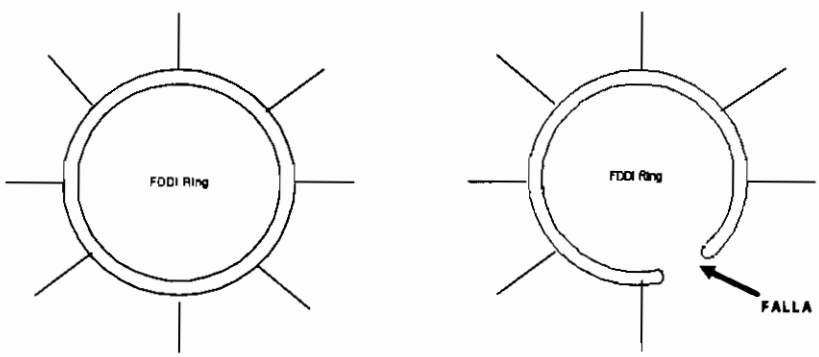


Figura 1.10 Topología física en anillo doble

La redirección hace que las transmisiones duren más, pero evita dejar dispositivos aislados.

Ventajas	Inconvenientes
Fallas en el cable pueden determinarse fácilmente.	Más difíciles de instalar y configurar que la topología en bus
Los anillos de doble bucle pueden ser muy tolerantes a fallos	En caso de un fallo en el medio para una topología en anillo con un único bucle, todas las estaciones se ven afectadas.

Tabla 1.3 Ventajas e inconvenientes de la topología física en anillo

c. Topología radial

Los ETDs están unidos mediante cables de tendido a un dispositivo central denominado hub, concentrador o repetidor multipunto. El concentrador guarda una relación de enlace punto a punto con cada uno de los ETDs. Las topologías radiales pueden estar anidadas unas dentro de otras, formando una estructura jerárquica o en árbol.

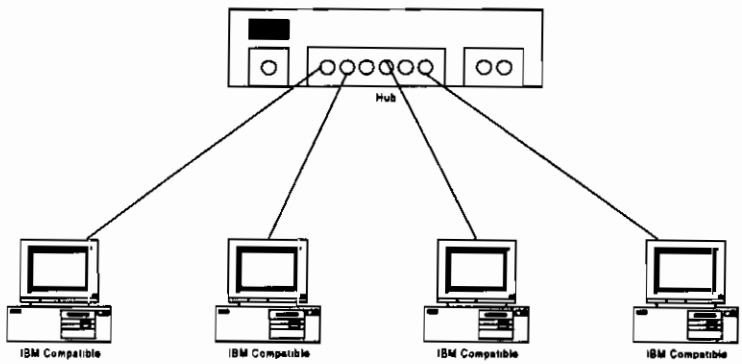


***Figura 1.11** Topología física radial*

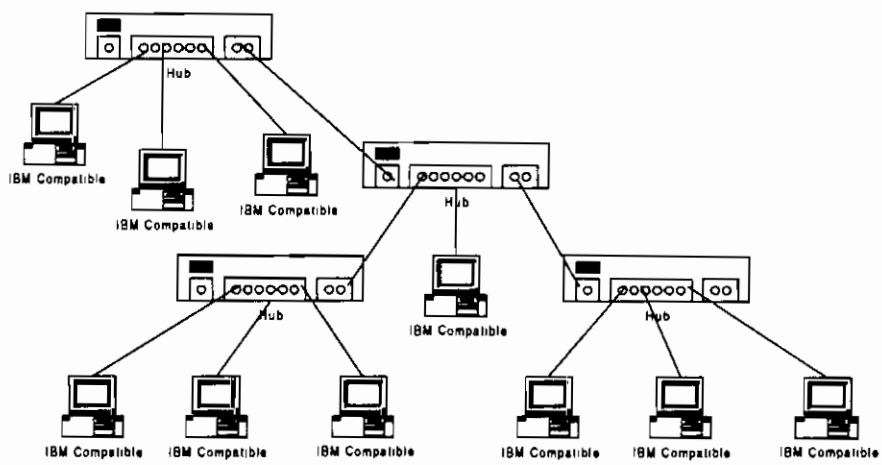


***Figura 1.12** Topología física radial anidada*

Ventajas	Inconvenientes
Relativamente fácil de reconfigurar	Requiere más cable que otras topologías
Facilidad para localización de averías	Instalación poco complicada.
La tolerancia a fallos es alta. El daño se reduce por lo general al segmento de uno de los cables de tendido	

***Tabla 1.4** Ventajas e inconvenientes de la topología física radial*

d. Topología combinada

También conocida como topología de malla, mantiene conexiones punto a punto entre cada uno de los dispositivos y la red. Dentro de esta topología, son reconocidos dos tipos:

- Malla auténtica
- Malla híbrida

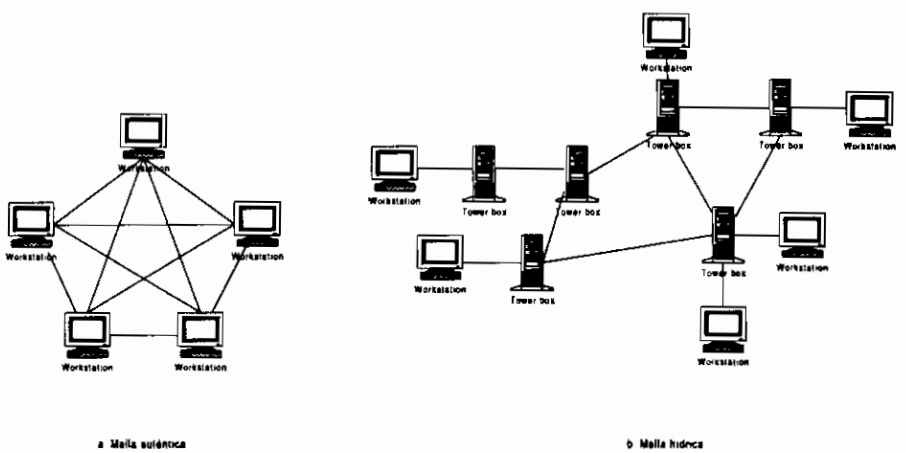


Figura 1.13 Topología física en malla e híbrida

Las topologías combinadas no suelen ser prácticas porque a menos que se utilicen protocolos complicados de control de tráfico, utilizan un excesivo ancho de banda. Esta topología se utiliza en enlaces de WAN (triangulación), donde se requiere una extremada tolerancia a fallos.

Ventajas	Inconvenientes
Facilidad para localización de averías	Dificultad para instalación y reconfiguración
Tolerancia a fallos extremadamente alta	

Tabla 1.5 Ventajas e inconvenientes de la topología física combinada

e. Topología celular

La topología celular divide el área geográfica en células combinando estrategias punto a punto y multipunto. Cada célula representa una parte de toda el área de la red dentro de la cual funcionan los dispositivos que se encuentran en esa área. Cada área tiene su concentrador y se comunican a las estaciones como en la topología multipunto. Las áreas se

comunican entre sí logrando la comunicación de los concentradores a través de enlaces punto a punto. Se habla de áreas, debido a que en este tipo de topología se hace referencia a un medio sin cable, en el cual cada concentrador tiene cobertura sobre su área y las estaciones pueden movilizarse libremente dentro de su área inicial o cambiando su posición a otra.

Ventajas	Inconvenientes
Facilidad de instalación	Si falla el concentrador fallarán todos los dispositivos conectados a él
No requiere reconfiguración cuando se añaden o trasladan equipos	
El aislamiento y localización de averías son relativamente sencillos	

***Tabla 1.6** Ventajas e inconvenientes de la topología física celular*

B.3 Modulación o señalización digital y modulación o señalización analógica

La señalización es el proceso de envío de una señal de transmisión sobre un medio físico con propósitos de comunicación.

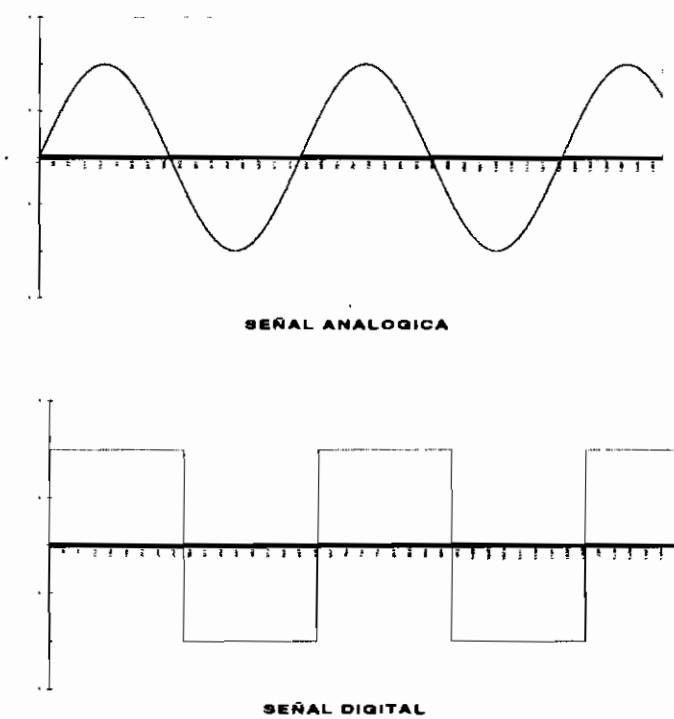


***Figura 1.14** Señales analógicas y digitales*

La señalización puede ser de dos tipos: digital y analógica. Los dos tipos de señalización representan datos mediante la manipulación de características eléctricas o electromagnéticas. La forma en que cambian dichas señales o estados determinan si una señal es digital o analógica. Las señales analógicas se representan mediante estados continuos, mientras que la señalización digital utiliza estados discontinuos.

Una señal digital es aquella señal cuantizada en amplitud y duración. La transmisión de datos se hace posible gracias a señales cuantizadas en amplitud pero con duraciones fijas.

El número de amplitudes viene dado por 2^n, donde n es el número de bits que serán representados por un estado. Es decir, si por ejemplo se tienen 8 amplitudes, cada amplitud (estado) puede representar la combinación de 3 bits.

La velocidad de transmisión (V_{tx}) viene dada por el producto entre el número de bits representados por estado (n) y la velocidad de modulación (V_m). La velocidad de modulación se define como el número de señales o estados que se envían al medio de transmisión por unidad de tiempo.

$$Vtx = n \cdot Vm$$

donde: Vtx es la velocidad de transmisión
n es el número de bits por estado
Vm es la velocidad de modulación

Las unidades para V_{tx}, n y V_m son: bits/s, bits/señal y señales/s (baudios) respectivamente. En el caso de la señal binaria, el número de bits por señal es uno, y existen solo dos estados (0 ó 1). Por tanto en este caso el módulo de la velocidad de transmisión es igual al de la velocidad de modulación.

En la transmisión de datos basta con muestrear la señal en determinados instantes para verificar cuál es su valor cuantificado sin que interese su reconstrucción completa.

Las señales analógicas se basan en estados continuadamente variables de las ondas eléctricas ó electromagnéticas. Una señal analógica está definida por tres características fundamentales: amplitud, frecuencia y fase.

$$S(t) = A \cos (W_c t + \Theta)$$

donde: A define la amplitud
W_c define la frecuencia
Θ define la fase

Señalización digital	Señalización analógica
En señalización digital el equipo suele ser más barato y sencillo	La señalización analógica admite técnicas de multiplexión que pueden maximizar el uso del ancho de banda
La señalización digital tiene menos errores debidos al ruido y a interferencias	La señalización analógica tiene más errores por el ruido e interferencias que la señalización digital
En enlaces de larga distancia, debido a la regeneración de la señal, es posible eliminar ruidos e interferencias	En enlaces de larga distancia, la regeneración de la señal comprende también la de ruido e interferencia
En general ocupa mayor ancho de banda que la señal analógica	Ocupa menor ancho de banda con relación a la señal digital

Tabla 1.7 Comparación entre la señalización digital y señalización analógica

B.4 Sincronización de bits

Se sabe que para la transmisión de datos a través de una determinada infraestructura de transporte, los datos necesitan ser adecuados, bien sea con técnicas de modulación digital o analógica. Cuando estas señales llegan a su destino, aquellas necesitan ser interpretadas por los receptores. Para cumplir con este objetivo, el receptor toma una medida de las características de la señal modulada que más interesa, por tanto el receptor debe saber el momento exacto en que se debe tomar la medida de esa característica para obtener los datos sin errores de demodulación o decodificación.

El control de los relojes de sincronización de mediciones se llama sincronización de bits. Existen dos tipos de sincronización de bits:

- Asincrónico
- Sincrónico

Toda transmisión de datos requiere de uno de los dos tipos de sincronización de bits, y por tanto es un factor que debe considerarse durante la transferencia de datos, pues cada método requiere de una cantidad distinta de ancho de banda y de recursos del medio.

Técnicas de sincronización de bits

a. Asincrónico

El método de sincronización de bits asincrónico utiliza señales intermitentes para transmitir los bits. Cuando no se transmiten datos, no se producen cambios en el estado de la señal en el medio. Una vez que se transmiten datos, los dispositivos utilizan un reloj interno de *hardware* para saber con qué frecuencia deben medir la señal.

Los dispositivos transmisores y receptores logran ponerse de acuerdo gracias a señales de control que se envían entre ellos. El dispositivo transmisor envía un bit de inicio antes de transmitir los datos y el dispositivo receptor activa su reloj interno para recibir la señal. Una vez que el transmisor termina de enviar los datos, aquel envía un bit final o de parada para indicar el fin de la transmisión al receptor. De esta forma, se observa que una transmisión asincrónica de datos se realiza únicamente cuando hay datos que transmitir.

b. Sincrónico

A diferencia del método anterior, en el método sincrónico, se producen flujos continuos de bits sincrónicos para proporcionar un reloj que sincroniza los relojes de los dispositivos que transmiten y reciben datos. Normalmente se utilizan tres técnicas:

1. Cambio de estado garantizado
2. Señales de reloj diferentes
3. Sobremuestreo

b.1 Cambio de estado garantizado

Esta técnica de temporización utiliza una señal de reloj incorporada a la señal de datos. De esta forma se garantiza que la señal de transmisión sufrirá una transición en un intervalo de tiempo predeterminado. El receptor espera este cambio y ajusta continuamente su reloj interno.

Aplicación: Esta técnica se suele utilizar con las señales digitales en enlaces de larga distancia.

b.2 Señales de reloj diferentes

Esta técnica utiliza dos canales de transmisión. En uno de ellos se transmiten los datos, mientras que en el otro se envía la señal de reloj. Este método requiere un canal exclusivo para la señal de reloj, por tanto "desperdicia" ancho de banda. En grandes distancias es fácil perder la sincronización entre la señal de datos y la de reloj.

Aplicación: Está técnica es muy eficaz en transmisiones de distancias cortas, como las que se usa a través del interfaz RS-232.

b.3 Sobremuestreo

En esta técnica, el receptor muestrea la señal a una velocidad mucho mayor que la velocidad de datos. Debido a que los relojes de emisor y receptor tienden a perder la sincronización lentamente, el sobremuestreo indica cuándo se deben efectuar ajustes en el reloj receptor.

Aplicación: En sistemas de transmisión con multiplex PDH (jerarquía digital plesiócrono).

B.5. Uso del ancho de banda

El término ancho de banda hace referencia a la capacidad de un medio de transmisión, cuanto mayor sea el ancho de banda, mayor será la capacidad de transmisión de datos. Un ancho de banda puede contener uno o varios canales de transmisión de datos. Un *canal* es una parte del ancho de banda total del medio, el cual se crea dividiendo las múltiples frecuencias electromagnéticas que puede admitir un medio.

Se tienen básicamente dos técnicas de uso del ancho de banda:

- Banda base
- Banda ancha (Broad band)

La capacidad de transmisión que el medio puede proporcionar depende de la técnica de uso del ancho de banda que utilice.

Técnicas de uso del ancho de banda

a. Banda base

Los sistemas de banda base se caracterizan por usar toda la capacidad del medio de transmisión para un único canal. Las redes de banda base pueden utilizar señalización analógica o digital, aunque la digital es la más común.

El que la señal utilice todo el ancho de banda que el canal le permite, no significa que varias señales no puedan ser multiplexadas, pues como se verá a continuación, a más de la multiplexación de frecuencia que es la que se utiliza en transmisiones en banda ancha, existe también la multiplexación en el tiempo. Esta última permite que una transmisión en banda base pueda suplir varias señales simultáneamente.

Por lo general, las señales de banda base pueden interpretarse y regenerarse de forma más confiable que las de banda ancha.

b. Banda ancha

Los sistemas de banda ancha utilizan la capacidad del medio de transmisión para proporcionar múltiples canales. La división de un único ancho de banda en múltiples canales de transmisión se consigue gracias a la multiplexación de frecuencia. Debe tomarse en cuenta que la transmisión de varias portadoras simultáneamente se consigue utilizando señales analógicas.

B.6 Multiplexión

La multiplexión es la técnica que permite compartir a varias señales el mismo medio de transmisión. Utilizando la multiplexión pueden crearse múltiples canales en un único medio de transmisión.

Los multiplexores, permiten agrupar varios canales en un solo medio. Basta que la suma del ancho de banda de todos los canales sea igual o menor que el ancho de banda máximo que soporta el medio.

Técnicas de multiplexión

Se conocen tres técnicas básicas de multiplexión:

a. Multiplexación por división de frecuencias (FDM)
b. Multiplexación por división de tiempo (TDM)
c. Multiplexión estadística de división de tiempo (STDM)

a. Multiplexión de división de frecuencia

Esta técnica divide el ancho de banda de frecuencias en varios canales, utilizando múltiples portadoras para este efecto. Las señales de datos se añaden en las portadoras.

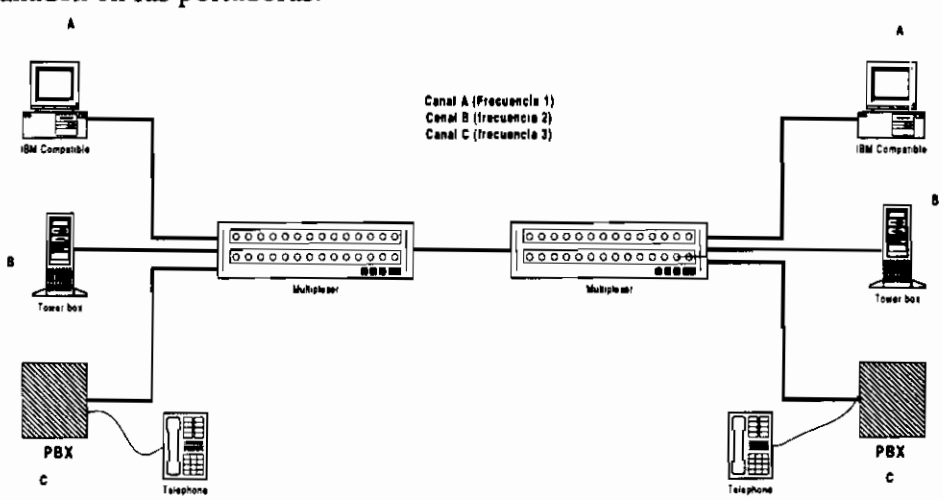


Figura 1.15 Multiplexación de división de frecuencia

Aplicación: Se utilizan en LAN de banda ancha para separar el tráfico de distinta dirección dentro del cable y proporcionar servicios especiales tales como las conexiones dedicadas entre máquinas.

b. Multiplexión de división en el tiempo

La técnica de multiplexión por división en el tiempo, no utiliza varias portadoras, sino que asigna intervalos de tiempo a varias señales siguiendo una secuencia determinada. De esta manera consigue utilizar un único canal para varias señales. Los intervalos de tiempo asignados tienen longitud constante y se asignan en el mismo orden. A esta técnica se la conoce también como TDM sincrónica.

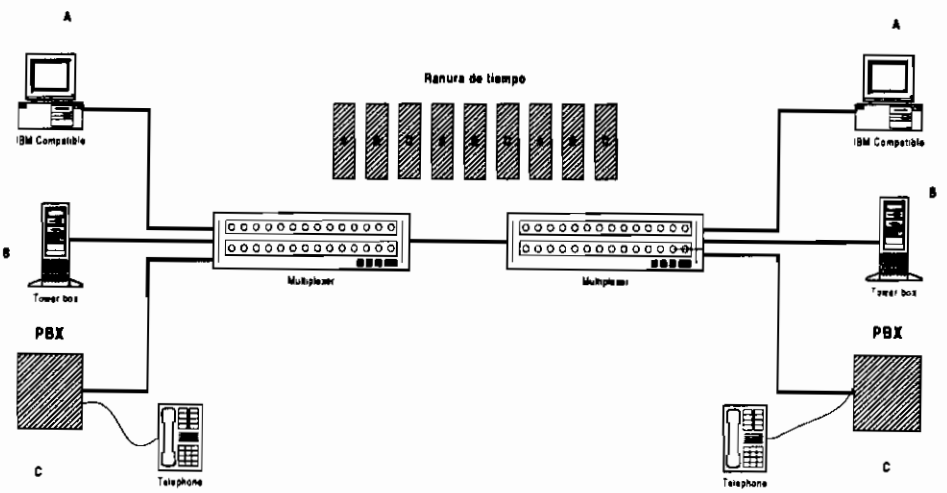


***Figura 1.16* Multiplexación de división en el tiempo**

Aplicación: Debido a que utiliza un único canal de comunicación dentro del medio disponible, la multiplexión TDM puede ser utilizada en sistemas de banda base.

En algunas aplicaciones puede aplicarse TDM dentro de un único canal de FDM.

c. Multiplexión estadística de división en el tiempo

La tradicional técnica TDM sincrónica no aprovechan al máximo el ancho de banda disponible, especialmente si existen muchos intervalos de tiempo sin utilizar. Tratando de eliminar este desperdicio de ancho de banda, se creó la técnica TDM estadística. Esta última asigna intervalos de tiempo priorizando los requerimientos de utilización del canal de acuerdo con determinadas estadísticas.

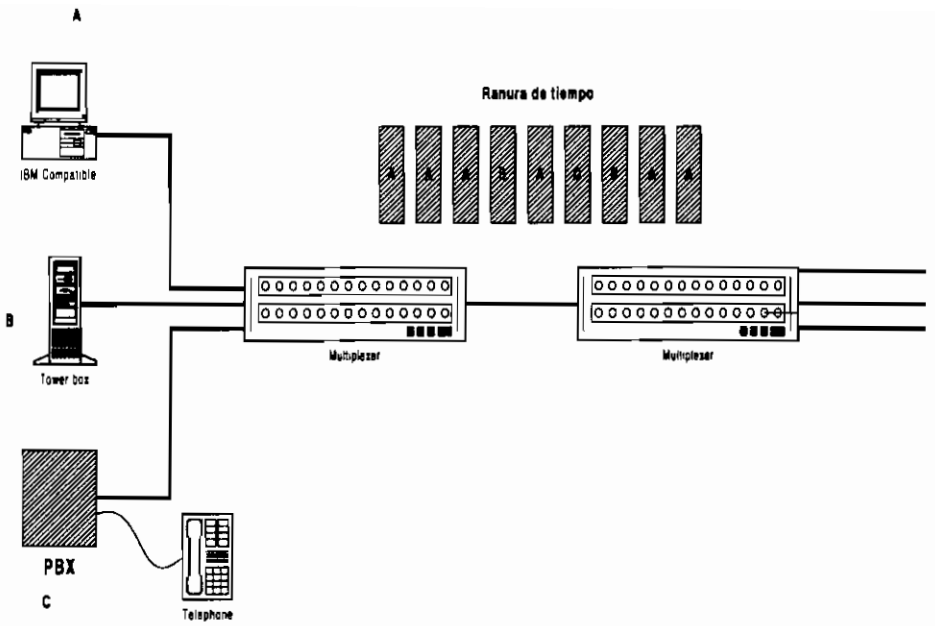


Figura 1.17 Multiplexación estadística de división en el tiempo

1.2.5.2 El nivel enlace de datos OSI

Las unidades de datos en este nivel son conocidas como tramas. Los propósitos básicos del nivel enlace de datos son los siguientes:

- Organizar los bits del nivel físico en grupos lógicos de información denominados *tramas.*
- Detectar y en algunos casos corregir errores.
- Controlar el flujo de datos.
- Identificar a las computadoras de la red.

El nivel enlace de datos añade su propia información de control como cabecera del paquete de datos. La cabecera contiene por lo general información del *hardware* de origen y destino, información sobre la longitud de la trama e indicación de los protocolos de nivel superior.

A. *Hardware* de conectividad de red asociado con el nivel enlace de datos OSI

Los dispositivos de conectividad de red asociados con el nivel enlace de datos son:

1. *Bridges* o puentes:

   Función: Pasar los paquetes entre dos segmentos de red.

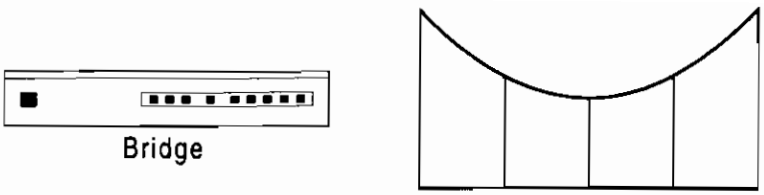


Figura 1.18 Puente y su representación típica

2. Concentradores inteligentes:

Función: Es la misma que la de los concentradores simples, pero además éstos permiten tener administración, son más resistentes a fallos y determinan automáticamente cuando uno de sus puertos tiene problemas, cerrando ese camino.

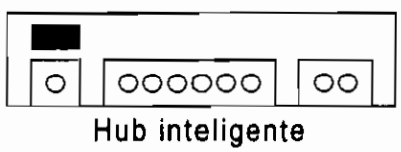


Figura 1.19 Hub o concentrador inteligente

3. Tarjetas de interfaz de red (NIC-Network Interface Card):

Función : Transformar la señal que llega del medio de transmisión en datos entendibles por el computador y viceversa.

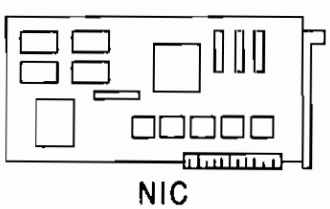


Figura 1.20 Tarjeta de interfaz de red

B. Temas y técnicas del nivel enlace de datos OSI

Los temas y técnicas utilizados en este nivel se resumen en la tabla 1.8.

Las funciones del nivel enlace de datos se subdividen en dos subniveles:

1. Control de acceso a medios (MAC)
2. Control de enlace lógico (LLC)

Nivel OSI	Temas	Técnicas
Enlace de Datos-MAC	Topología lógica	Bus Anillo
	Acceso a medios	Contención (*Contention*) Entrega de testigo Sondeo (*Polling*)
	Direccionamiento	Dispositivo Físico
Enlace de datos-LLC	Sincronización de transmisiones	Asincrónico Sincrónico Isocrónico
	Servicios de conexión	Control de flujo a nivel LLC Control de errores

Tabla 1.8 Temas y técnicas del **nivel enlace** *de datos OSI*

B.1 Enlace de datos - MAC (Control de acceso a medios)

Este subnivel se encarga de controlar la forma en que los transmisores comparten un canal de transmisión único. Sus funciones se describen con más detalle en el tema acceso a medios que se encuentra más adelante.

B.1.a Topología lógica

Anteriormente ya se trató el tema referente a la topología física del primer nivel del modelo de referencia OSI, a la que se hizo referencia como la estructura del medio o recorrido de los datos. Para ser más descriptivos, la topología física tendrá que ver con la forma que adopta físicamente tanto la infraestructura de transporte (cableado) y el subsistema de conectividad. Sin embargo, la topología física no siempre reflejará la forma en que funciona la red, pues las entidades de la red transmiten los datos en función de la topología lógica de la red. El recorrido real de la señal de datos se denomina topología lógica.

Un ejemplo que clarifica la diferencia entre la topología lógica y la topología física son las redes *Token*-Ring. Si bien su topología física es radial, su topología lógica es en anillo, pues el testigo va pasando de computador en computador y no como debería ser en la topología radial: del concentrador a todas los dispositivos conectados a él.

Tipos de topología lógica

La topología lógica utilizada en una red depende de la forma en que se *reciben* las señales.

a. Topología lógica en bus

En este tipo de topología todos los dispositivos reciben simultáneamente cada una de las señales.

b. Topología lógica en anillo

En este tipo de topología cada dispositivo recibe sólo las señales que se le envía exclusivamente.

B.1.b Acceso a medios

El acceso a medios es un proceso de control que utiliza normas específicas para que las topologías lógicas puedan organizar la transmisión de las señales de datos de cada uno de sus dispositivos.

Si no existieran las normas de acceso a medios que se mencionó, los dispositivos conectados a una red no podrían comunicarse, pues las colisiones o choques que se producirían por transmisiones simultáneas de varios equipos sería tan grande que la red no funcionaría. Si se hace una analogía con un grupo de estudiantes en una aula de clase, se vería que cuando un alumno desea intervenir, aquel levantará la mano y luego de habérsele concedido la palabra, intervendrá. Si esto no sucediera y todos hablarían al mismo tiempo sería prácticamente imposible la comunicación, o en el mejor de los casos sumamente deficiente.

a. Factores importantes en la elección de una técnica de acceso a medios

Antes de seleccionar un protocolo que implemente una de estas técnicas de acceso a medios, deberían considerarse los siguientes factores:

1. La naturaleza coherente o en ráfagas de las transmisiones. Esto es importante para definir si los dispositivos requieren del medio por períodos continuos de tiempo (más o menos constantes), ó pueden disponer de un tipo de acceso probabilístico.
2. La cantidad de transmisiones de datos. Con la técnica de sondeo para acceder al medio, el protocolo limita la cantidad de datos que pueden transmitir cada uno de los secundarios.
3. El tiempo de respuesta requerido. Es importante calificar la sensibilidad de los datos frente al tiempo. En aplicaciones multimedia por ejemplo es recomendable paso de testigo (*Token Passing)* como método de acceso, sin embargo debido a que actualmente se disponen de medios que permiten transmisiones de 100 Mbps con método de acceso de contención (100BaseT por ejemplo), este factor debe considerarse en combinación con la velocidad de transmisión de la red. En general para equipos de automatización se recomienda el método de sondeo para el acceso al medio cuando los datos son sensibles al tiempo.

4. El número de dispositivos activos en la red. Este factor se considera debido a que el rendimiento con carga elevada es mejor con *Token-Ring* como método de acceso a medio, mientras que para condiciones de poca carga el método de contención es más recomendable.

b. Técnicas de acceso a medios

Para evitar las colisiones producidas por la aleatoriedad de transmisiones de los dispositivos de una red, se han creado técnicas que se utilizan para garantizar un acceso a medios organizado. Las siguientes son técnicas o métodos de acceso a medios:

a. Contención (*contention*)
b. Entrega de testigo (*token*)
c. Sondeo (*polling*)

b.1 *Contention*

En la técnica de contención, todos los dispositivos conectados a la red tratan continuamente de obtener el acceso al medio. Es decir, cada uno de los dispositivos compite por obtener el control del medio. Esta práctica genera colisiones cuyo número aumenta en progresión geométrica al número de dispositivos. Debido a que el acceso al medio depende de la probabilidad de encontrarlo libre, los tiempos de acceso al medio no son predecibles, son probabilísticos.

Para reducir el número de colisiones, se han desarrollado nuevos protocolos de contención que obligan a los dispositivos conectados a la red a detectar si existen otros dispositivos que estén utilizando el medio. Esto protocolos se denominan protocolos de detección de portadora y acceso múltiple (CSMA). Aunque los protocolos CSMA disminuyen el número de las colisiones, no las eliminan. Las estaciones verifican la existencia o la ausencia de portadora en el medio, si no existe portadora entonces toman control del medio, sino esperan hasta que se desocupe. Las colisiones se presentan cuando dos dispositivos hacen la detección al mismo tiempo y verifican que no existe portadora, a continuación transmiten simultáneamente, lo que genera colisión.

Dos tipos conocidos de técnicas de detección de portadora se nombran a continuación:

- Detección de portadora y acceso múltiple/detección de colisiones (CSMA/CD). Los protocolos que usan esta técnica no sólo hacen detección de portadora, sino que además detectan colisiones e inician retransmisiones.
- Detección de portadora y acceso múltiple/evita colisiones (CSMA/CA). Los protocolos que utilizan esta técnica utilizan

programas como el acceso o peticiones con división de tiempo para acceder al medio.

Dentro de protocolos conocidos que utilizan contención como método o técnica de acceso al medio se tienen los siguientes:

- El estándar IEEE 802.3 es un ejemplo de protocolo que utiliza CSMA/CD.
- El protocolo LocalTalk de Apple Computer utiliza CSMA/CA.

Aplicaciones:

El método de acceso al medio por contención es apropiado para redes en donde existe tráfico en ráfagas (como la transferencia intermitente de archivos extensos) en redes poco pobladas o de cargas no muy elevadas

Ventajas	Inconvenientes
El *software* es relativamente sencillo y exige pocos recursos a servicios. Esto refleja que su precio comparativo es bajo.	Los tiempos de acceso son impredecibles por lo que se les denomina probabilísticos
Se tiene un control inmediato y completo del medio, mientras no tenga acceso al medio otro dispositivo	No pueden utilizarse prioridades para proporcionar un acceso más rápido a algunos dispositivos que lo requieren
	Las colisiones aumentan en progresión geométrica cuando se añaden nuevos dispositivos. Es decir su rendimiento disminuye ante condiciones elevadas de carga.

***Tabla 1.9* Ventajas e inconvenientes de contención**

b.2 Entrega de testigo

Los protocolos que utilizan este método de acceso al medio utilizan una pequeña trama de datos denominada testigo que se entrega de forma ordenada de un dispositivo a otro. El testigo es un mensaje especial que proporciona al dispositivo que lo retiene un control temporal del medio. El testigo se va asignando a todos los dispositivos de la red uno por uno. Podría relacionarse con una "licencia" que se va entregando a cada dispositivo para que pueda mantener el control temporal del medio en su turno.

Cada dispositivo sabe de quien recibe el testigo y a qué dispositivo debe entregarlo. Cada dispositivo toma control del testigo periódicamente, y luego de haber realizado lo que requería pasa el testigo a otro dispositivo.

Los protocolos limitan cuánto tiempo puede controlar el testigo cada dispositivo.

Se disponen de varios protocolos de entrega de testigo. Dentro de los estándares de LAN en cuanto a entrega de testigo se tienen el IEEE 802.4 *Token Bus*, el IEEE 802.5 *Token-Ring* y el estándar X3T9.5 de ANSI[4] para FDDI (*Fiber Distributed Data Interface*).

- La red *Token* bus utiliza como método de acceso al medio la entrega de testigo y una topología física y lógica en bus.
- El estándar *Token-Ring* utiliza entrega de testigo pero sobre una topología física en estrella y lógica en anillo.
- FDDI utiliza entrega de testigo sobre una topología física de doble anillo y topología lógica en anillo. El doble anillo de la topología física es para garantizar tolerancia a fallas. Este estándar define un dual *Token-Ring* trabajando a 100 Mbps sobre fibra óptica.

Aplicaciones :

Los protocolos que utilizan entrega de testigo son recomendables para redes con un tráfico muy sensitivo al tiempo o con prioridades establecidas, tales como las de voz digital o de video y en redes muy pobladas.

Ventajas	Inconvenientes
La entrega de testigo produce demora y carga predecible por lo que se denomina determinística.	Requiere *software* interactivo relativamente complicado en todos los dispositivos que deben ser razonablemente inteligentes, por tanto la implementación es relativamente costosa.
Tiene la posibilidad de asignar niveles de prioridad a las transmisiones de datos, garantizando un acceso al medio más eficiente y fiable.	Se deben ajustar los parámetros de *software* de los dispositivos cada vez que se añaden o eliminan dispositivos.
Es eficiente en condiciones de carga elevada debido a que elimina las colisiones.	Algunos requieren de un controlador central adicional para la detección y recuperación de fallos.

***Tabla 1.10* Ventajas e inconvenientes de entrega de testigo**

[4] Estándar referido al paso de testigo para velocidades de 100 Mbps (FDDI, CDDI cumplen con este estándar)

b.3 Sondeo

En esta técnica o método de acceso al medio se definen dos tipos de dispositivos: un primario y el resto secundarios. El dispositivo primario (controlador o maestro) se encarga de administrar el acceso al medio. Este dispositivo se encarga de preguntar en un determinado orden a cada uno de los dispositivos secundarios si tienen información para transmitir. Para obtener la información del secundario, el primario emite una petición de datos al secundario y luego recibe los datos que éste le envía. Posteriormente el primario sondea al próximo secundario definido en orden, solicita su información y así sucesivamente. En esta técnica, el protocolo limita la cantidad de datos que pueden transmitir cada uno de los secundarios luego de cada sondeo.

Protocolos conocidos que utilizan sondeo:

- SDLC (*Syncronous Data Link Control*) que es un protocolo de comunicaciones de datos de bit sincrónicos desarrollado por IBM.

Aplicaciones:

Los protocolos que utilizan sondeo como técnica de acceso al medio son recomendables en aplicaciones sensibles al tiempo, tales como equipos de automatización.

Ventajas	Inconvenientes
Tiene control de acceso al medio centralizado, por lo que hace más fácil su administración.	Pueden generarse demoras que para ciertas aplicaciones no sean aceptables, debido a que los dispositivos secundarios deben esperar hasta que el primario les pregunte si tienen datos.
Debido a que pueden generarse estadísticas de valores máximos y mínimos para los tiempos de acceso y velocidades de datos, puede considerarse como un método determinístico.	Utiliza ancho de banda en avisos y reconocimientos o recibiendo mensajes.
Permite que se asignen niveles de prioridad para garantizar un acceso más rápido.	Implica más recursos a servicios que otros métodos de acceso a medios.
Elimina las colisiones, permitiendo una completa utilización del medio.	

***Tabla 1.11** Ventajas e inconvenientes de sondeo como técnica de acceso a medios*

B.1.c Direccionamiento

El direccionamiento permite que se puedan diferenciar o distinguir a los distintos dispositivos de la red.

Una analogía para describir el direccionamiento sería el servicio de correos. Para entregar el correo en el sitio correcto, el cartero debe tener el número de casa, la calle, la ciudad y el país. Pueden en algunos casos utilizarse códigos postales que simplifican la dirección de un destino. De la misma forma, el direccionamiento en las redes de computadores se utilizan números o nombres de proceso de *software*, dispositivos físicos o redes para definir una dirección exclusiva a cada uno de los dispositivos de la red. En algunos casos, se pueden asociar otros nombres o números lógicos que simplifiquen la dirección.

De manera general se conocen tres tipos de direccionamiento:

1. Utilizando las direcciones MAC (usado por el nivel enlace de datos).
2. Utilizando direcciones de red lógica (usado por el nivel red)
3. Utilizando direcciones de servicios (usado por nivel red)

En este nivel se hará referencia solamente al direccionamiento utilizando las direcciones MAC. Los otros dos tipos de direccionamiento se verán en la parte correspondiente al nivel red.

Técnica de dispositivo físico (Direcciones MAC)

- Para que múltiples estaciones puedan compartir el mismo medio y permitir que se identifiquen unas de otras, en esta subcapa se define una dirección de *hardware* llamada dirección MAC.

En las tarjetas de interfaz LAN, la dirección MAC es incluida dentro de la ROM, de aquí el término *burned-in-address* (BIA). Cuando la tarjeta de interfaz de red inicializa, esta dirección es copiada a la RAM.

El nivel enlace de datos tiene relación solamente con las direcciones de dispositivo físico, llamadas también direcciones MAC. Las direcciones MAC son direcciones de *hardware* exclusivas que las asignan sus proveedores; estos últimos utilizan las direcciones que les asignan las organizaciones de normalización. El formato depende del método de acceso a medios que utilice, por este motivo el nombre de direcciones MAC (*Media Access Control*).

La dirección MAC es una dirección de 48 bits expresada como 12 dígitos hexadecimales. Los primeros 6 dígitos hexadecimales de una dirección MAC contienen la identificación del fabricante (código del vendedor) también conocida como identificador único organizacional (OUI). Para garantizar que las direcciones provistas no se repitan, el Instituto de Ingenieros Eléctricos y Electrónicos (IEEE) administra los OUIs. Los últimos 6 dígitos hexadecimales

son administrados por cada proveedor y frecuentemente representan el número serial de la interfaz.

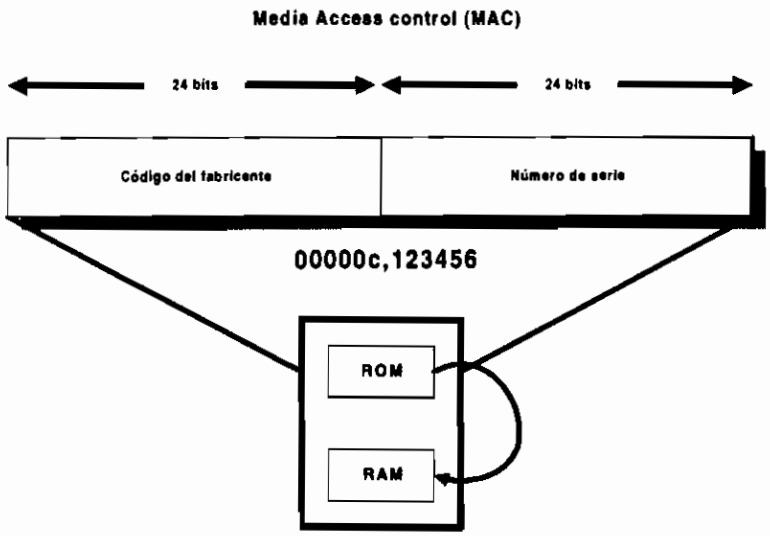


Figura 1.21 Representación de una dirección MAC y sus 12 dígitos hexadecimales

Antes de que una trama sea intercambiada con un dispositivo conectado directamente, el dispositivo de envío necesita tener una dirección MAC para usarla como dirección de destino. Una forma para descubrir una dirección MAC de un dispositivo es usar un protocolo de resolución de direcciones. La figura siguiente ilustra dos formas de usar un ARP (de TCP/IP) para descubrir una dirección MAC.

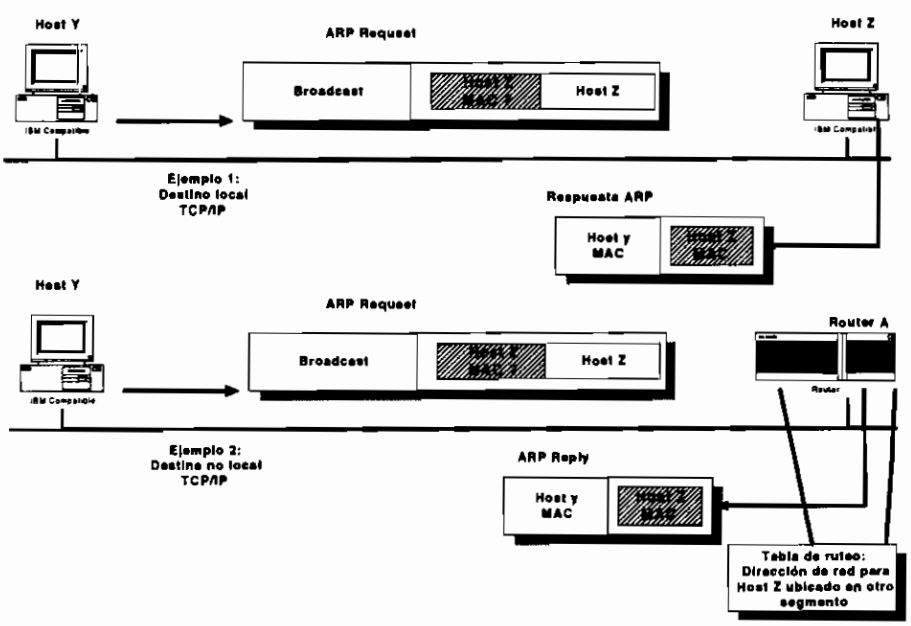


Figura 1.22 Descubrimiento inicial de direcciones MAC

En el primer ejemplo, el *host* Y y el *host* Z están sobre la misma LAN. El *host* Y envía un requerimiento ARP a toda la LAN buscando por Z. Todos los dispositivos reciben el mensaje (*broadcast*) pero solamente Z responde con su dirección MAC. El *host* Y recibe la respuesta de Z y graba la dirección MAC en la memoria local, frecuentemente llamada *ARP cache*. La próxima vez que el *host* Y necesite comunicarse con el *host* Z, aquel llamará directamente a la dirección MAC de Z que tiene almacenada en su memoria.

En el segundo ejemplo, el *host* Y y el *host* Z están sobre LANs diferentes, las cuales pueden comunicarse gracias al ruteador A. Cuando el *host* Y envía un *broadcast* haciendo un requerimiento ARP, el ruteador A determina que el *host* Z no puede reconocer el requerimiento porque conoce que el *host* Z está sobre una LAN diferente. Debido a que el ruteador A determina que cualquiera paquete para el *host* Z debe ser retransmitido, el ruteador A provee su propia dirección MAC como una respuesta *proxy* al requerimiento ARP. El *host* Y recibe la respuesta del ruteador y graba la dirección MAC en su memoria caché ARP. La próxima vez que el *host* Y necesite comunicarse con el *host* Z, lo hará con la dirección MAC almacenada del ruteador. Las direcciones de dispositivo físico también utilizan los bridges o puentes para repetir de forma selectiva las señales de datos en segmentos diferentes del medio. Los *bridges* "aprenden" la ubicación de los dispositivos de la red y construyen tablas de parejas dispositivo/segmento.

Como se ha visto en los ejemplos anteriores, pese a que los dispositivos pueden identificarse mediante su dirección física, la entrega real de datos en la LAN se realiza transmitiendo una trama a todos los dispositivos. Cada dispositivo lee la dirección física de la trama y el dispositivo cuya dirección física coincide con la dirección de la trama recoge los datos. El resto de dispositivos ignoran el resto de la trama.

B.2 Enlace de datos - LLC (Logical Link Control)

Este subnivel se encarga básicamente de:

- Habilitar a las capas más altas para ganar independencia sobre el acceso al medio LAN.
- Permitir puntos de acceso a servicio (SAPs) a las subcapas de interfaz hacia funciones de capas más altas.
- Proveer conexión opcional, control de flujo y servicios en secuencia.

La subcapa LLC se encarga de proveer flexibilidad de interfaz. Los protocolos de capas más altos pueden operar autónomamente sin tener que recordar el tipo de medio LAN. Esta independencia ocurre porque, a diferencia de la subcapa MAC, LLC no está limitada a un protocolo MAC específico. Al contrario, la subcapa LLC puede depender de las capas más bajas para proveer acceso al medio.

Desde la perspectiva de las subcapas MAC más bajas, el proceso de punto de acceso a servicios (SAP[5]) provee una interfaz conveniente a las capas OSI superiores. Estas entradas SAP simplifican el acceso al canal compartido hasta el servicio de capa más alto identificados por las entidades SAP LLC.

Las opciones de la subcapa LLC incluyen soporte para conexiones entre aplicaciones corriendo sobre la LAN, control de flujo a la capa más alta por medio de códigos *ready/no ready,* y bits de control de secuencia.

B.2.a Sincronización de transmisiones

Una vez que el transmisor sabe cuando puede enviar las tramas de datos, el receptor debe saber cuándo recibir las tramas completas. En el "nivel físico OSI" se trató el tema referente a sincronización de bits como método para coordinar el envío y la recepción de bits. Sin embargo, la sincronización de bits sólo garantiza los intervalos de tiempo al nivel de bits, mas no de tramas.

Técnicas de sincronización de transmisiones

Las técnicas de sincronización de transmisiones al nivel de tramas son las siguientes:

a. Asincrónico
b. Sincrónico
c. Isocrónico

a. Asincrónico

Los dispositivos que utilizan esta técnica de sincronización de transmisiones manejan sus propios relojes internos. Los dos utilizan una sincronización horaria similar pero no sincronizan sus relojes.
Los dispositivos asincrónicos envían cada trama de forma "aleatoria" en el tiempo. Para lograr sincronizar esta llegada "aleatoria" de tramas, se utilizan *bits de inicio y de parada* para definir justamente el inicio y fin de una trama de datos. Los bits de inicio y de parada no sólo indican cuando el receptor debe medir la presencia de bits, sino que también indican el inicio y el fin del flujo de datos.

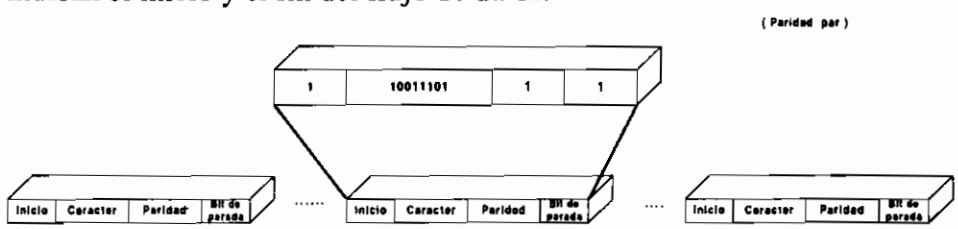


***Figura 1.23** Bits de inicio y parada en la transmisión asincrónica*

[5] En este caso SAP no se refiere al protocolo de notificación de servicios de Netware (Service Advertisement Protocol)

Resulta difícil que el receptor se equivoque en la detección del bit de inicio de la trama debido a que las cadenas de bits son relativamente cortas.

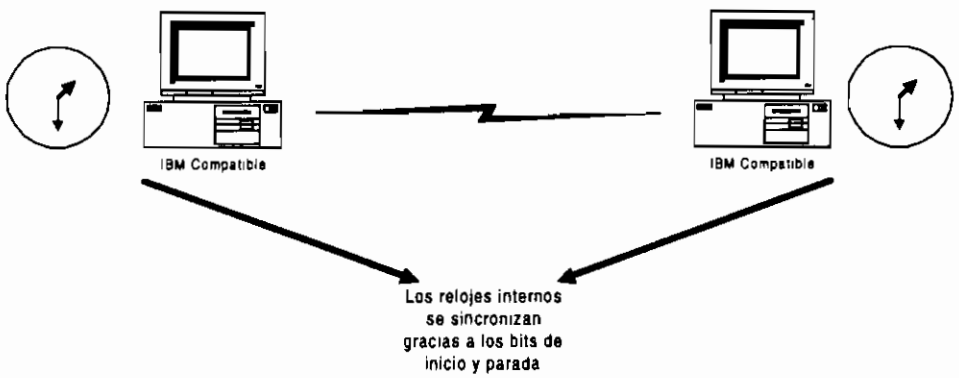


***Figura 1.24** Utilidad de los bits de inicio y parada en la sincronización de relojes en transmisión asincrónica*

Detección de errores:

Debido a su relativa sencillez, la detección de errores más comúnmente utilizada en transmisiones asincrónicas es el método denominado de paridad. Este método utiliza un bit de paridad al final de cada byte de la trama para indicar la paridad del byte.

Generalmente se habla de dos tipos de paridad: par e impar.

Aplicaciones:

Se utiliza esta técnica de sincronización de transmisiones especialmente en aplicaciones donde se generan caracteres a intervalos aleatorios, como por ejemplo los datos generados por el teclado de un terminal.

Ventajas	Desventajas
Utiliza tecnología sencilla y por tanto más económica	Dedica entre un 20 y 30 % de la trama a bits de control y corrección de errores
El método de detección de errores que se utilice puede ser sencillo	El método de detección de errores que por lo general utiliza (de paridad), puede ser vulnerado si se comete un número par de errores.
	Las transferencias son lentas si se compara con la transmisión sincrónica

***Tabla 1.12** Ventajas y desventajas de la técnica de sincronización asincrónica*

b. Sincrónica

Esta técnica permite mayores velocidades de transmisión que la asincrónica. En este método requiere que los dispositivos de comunicación asuman la responsabilidad del reloj de la transmisión. La sincronización del reloj puede conseguirse mediante las siguientes formas:

- Utilizando cadenas de bits de sincronismo (si está orientado a bits) ó utilizando uno o más caracteres de control (que suelen denominarse caracteres SYNC en sistemas orientado a caracteres).
- Utilizando otro canal dedicado para el reloj.

Los dos sistemas indican al receptor cuándo empieza una trama, para de esta forma organizar el momento en que necesita aceptar datos y a contar los bits para completar un byte o una trama.

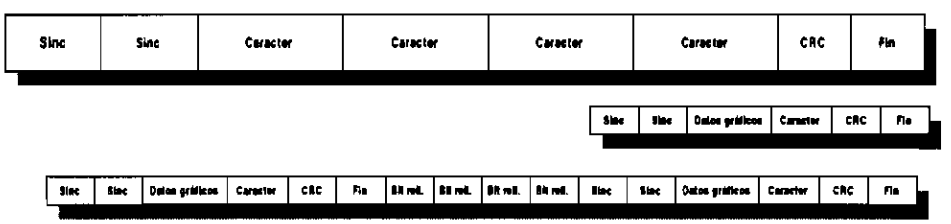


Figura 1.25 Bits de sincronismo en la transmisión sincrónica

Si bien las cadenas de bits en este tipo de transmisiones no son tan cortas como en la asincrónica, este tipo de transmisión resiste mucho mejor a los errores producidos por falta de sincronización en los relojes del transmisor y receptor, debido a que los dos utilizan el mismo reloj. La presencia de datos ayuda a mantener la sincronización en el reloj, sin embargo, cuando no existen datos a transmitir, se envían bits de relleno, que ayudan a mantener la sincronización.

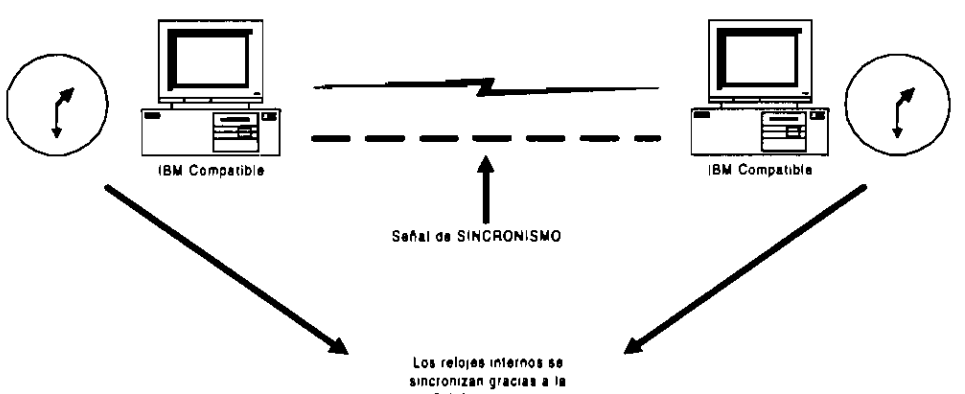


Figura 1.26 Utilización de bits de sincronismo para la sincronización de relojes en la transmisión sincrónica

Detección de errores:

El método de detección de errores que utiliza el tipo de transmisión sincrónica es por lo general denominado verificación de redundancia cíclica (CRC). El CRC es un proceso que asigna al bloque de datos un algoritmo. El resultado de este algoritmo (denominado CRC) es añadido al bloque de datos original. En el receptor se utiliza el mismo algoritmo y los resultados se comparan con el campo CRC. Si hay diferencias, significa que se han generado errores durante la transmisión. En el caso de producirse errores, podría pedirse retransmisión o utilizar un algoritmo más complejo que utilice el CRC para realizar la corrección de los errores.

Aplicaciones:

Este tipo de transmisión es frecuentemente utilizado para hacer transmisiones de bloques grandes de datos, pues eliminan gran parte del consumo de recursos que utiliza la asincrónica para bits de control y detección de errores.

Ventajas	Inconvenientes
Es más eficaz que la asincrónica, pues el porcentaje de uso de recursos para control y corrección de errores es relativamente pequeño.	Esta técnica es más compleja y por lo tanto más costosa.
Permite utilizar mayores velocidades de transmisión.	
Utiliza un mejor método de detección de errores	

***Tabla 1.13** Ventajas y desventajas de la técnica de sincronización sincrónica*

c. Isocrónica

En este tipo de transmisión se utiliza un reloj de transmisión con frecuencia fija para generar las ranuras de tiempo preestablecidas. Se genera una señal de reloj usando un dispositivo de red que se encargue de pasar dicha señal al resto de dispositivos.

Dentro de cada una de las ranuras establecidas se pueden insertar múltiples tramas. Debe notarse que con este tipo de transmisión, no se está utilizando una señal de reloj para cada trama (como en la asincrónica), ni se están enviando bits de sincronización al principio de la trama (como en la sincrónica). Aquí el reloj se proporciona a velocidad constante por un único dispositivo (que no necesariamente participa en la transferencia de datos) el cual transfiere su señal al resto de dispositivos.

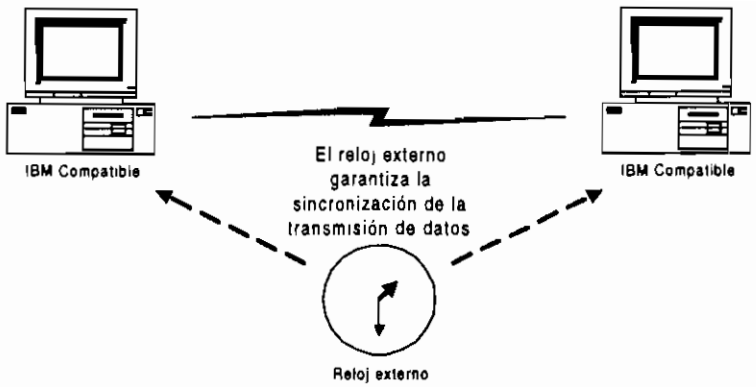


Figura 1.27 Sincronización de relojes entre extremos mediante la utilización de un reloj externo

Aplicaciones: Es generalmente utilizado en aplicaciones de distancias cortas.

Ventajas	Inconvenientes
Las velocidades de transmisión están garantizadas y son determinísticas.	Requiere de un mecanismo de temporización externo con tolerancia a fallos, que por lo general será costoso.
Requiere poquísimos recursos a servicios.	

Tabla 1.14 Ventajas y desventajas de la técnica de sincronización isocrónica

B.2.b Servicios de conexión

Existen 3 tipos de servicios de conexión:

1. **Servicios sin conexión y sin reconocimiento.** En esta técnica, el envío y recepción de tramas se los realiza sin control de flujo, errores o secuencias de paquetes.
2. **Servicios sin conexión y con reconocimiento.** En esta técnica, se utilizan los reconocimientos para conseguir control de flujo y de errores entre transmisiones punto a punto.
3. **Servicios orientados a conexión.** En esta técnica, el envío y recepción de tramas se los realiza con control de flujo, errores y secuencias de paquetes, mediante la utilización de reconocimientos. Los reconocimientos (ACK) son mensajes especiales que indican la recepción de una trama o paquete de datos.

Técnicas de control de servicios de conexión

Se conocen tres técnicas de control de servicios de conexión (control de flujo, control de errores y control de secuencias de paquetes), aunque al nivel enlace de datos LLC sólo se utiliza el control de flujo y de errores. Sin embargo, y en vista

de que en la capa de red y superiores se hace uso de las 3 técnicas, la descripción de éstas se muestra a continuación.

a. Control de flujo

El control de flujo permite controlar la cantidad de datos que se pueden transmitir entre dos entidades. Este tipo de control es importante debido a que la mayoría de redes están formadas por dispositivos que manejan diferentes velocidades de transmisión y distintas capacidades de procesamiento y almacenamiento. Los protocolos que utilizan control de flujo garantizan que los receptores más lentos puedan comunicarse con los más rápidos. Las normas de control de flujo determinan la cantidad de datos que se pueden transmitir dentro de un intervalo especificado.

El control de flujo regula los dispositivos que se encuentran a los dos lados de la comunicación y a los equipos intermedios. Es decir que en nuestro esquema, el control de flujo regula a los equipos ubicados en los subsistemas de equipos de aplicaciones y dispositivos de escritorio (dispositivos de los extremos) y al subsistema de conectividad (dispositivos intermedios).

Entre las formas de control de flujo más comunes se tiene:

- Control de flujo de ventana
- Control de flujo de velocidad garantizado

a.1 Control de flujo de ventana

El control de flujo de ventana utiliza un *buffer* (o ventana) en el que pueden colocarse un número establecido de tramas de datos. En este tipo de control de flujo de datos, los generadores y receptores de datos se van poniendo de acuerdo en el tamaño de ventana o *buffer* que van a utilizar durante la transmisión, dependiendo de las velocidades del transmisor y receptor.

En el control de flujo de ventana, existen dos estrategias de control de flujo:

- Control de flujo de ventana estático
- Control de flujo de ventana dinámico

En el **control de flujo de ventana estático,** el transmisor y receptor negocian un tamaño de ventana fijo durante la transmisión. El número de tramas pendientes permanece constante.

Supóngase que se utilice un tamaño de ventana que equivalga a 5 tramas, el transmisor enviará las tramas una por una pero numeradas en grupos de 5, asignando un número temporal de ventana a cada una de ellas. El receptor por su lado, irá recibiendo las tramas una por una y enviará un reconocimiento indicando que ha recibido la trama y que está preparada para recibir la siguiente. El transmisor podrá transmitir una nueva ventana o trama del siguiente grupo de 5, solamente si ha recibido confirmación de recepción de esa trama previamente numerada. Si no se recibiera el reconocimiento se procedería a la retransmisión de la ventana. De esta forma, se garantiza que no existan pendientes más de cinco tramas.

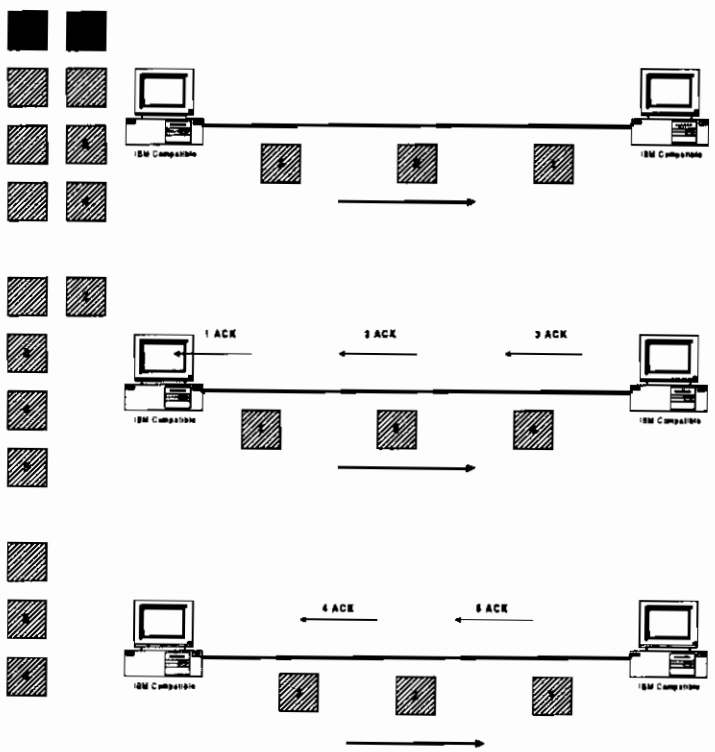


***Figura 1.28** Control de flujo de ventana estático*

En el **control de flujo de ventana dinámico,** el transmisor y receptor negocian un tamaño de ventana dinámico, flotante o deslizante durante la transmisión. Esto permite que los dispositivos de la red ajusten el tamaño de ventana para hacer la transmisión más eficiente. El número de tramas pendientes por tanto, varía de acuerdo al estado actual del receptor.

Cuando el *buffer* del receptor se satura, se envía al transmisor un paquete reductor (*choke package*) pidiéndole que las transmisiones sean más lentas. Una vez que el transmisor cumplió con el requerimiento del receptor, el transmisor empieza

a incrementar la velocidad de envío hasta que el receptor envíe nuevamente un paquete reductor. De esta forma el tamaño de la ventana aumenta y disminuye de tamaño constantemente.

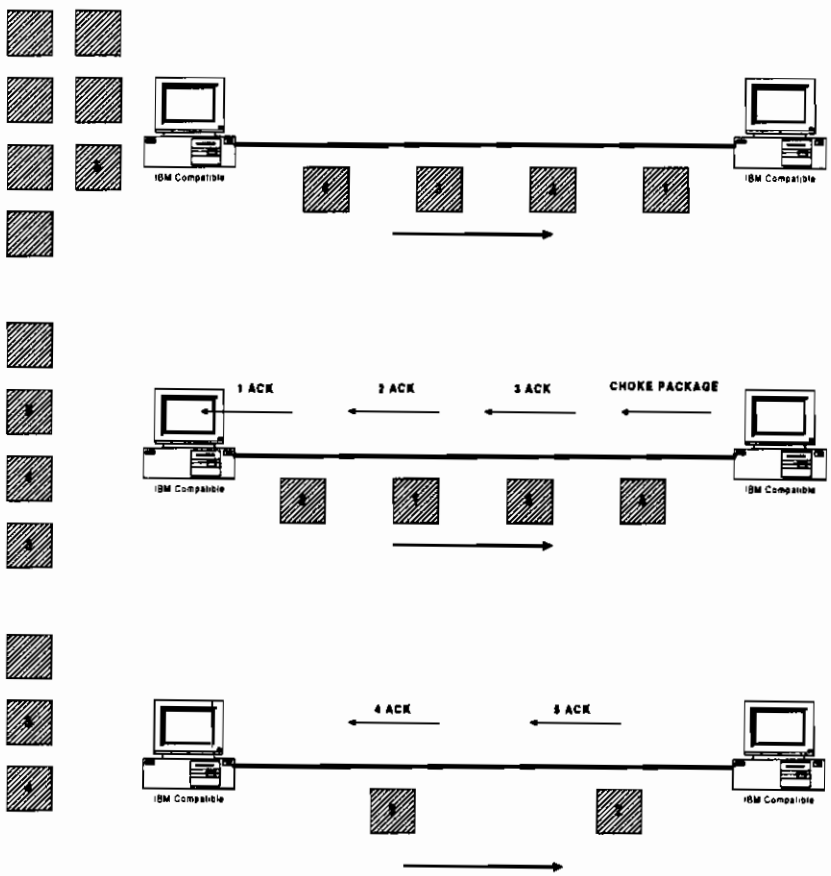


Figura 1.29 Control de flujo de ventana dinámico

a.2 Control de flujo de velocidad garantizado

En el control de flujo de velocidad garantizado el transmisor y receptor acuerdan y configuran una velocidad de envío de datos aceptable antes de que se hagan las transmisiones. Esta velocidad será respetada y garantizada durante esa conversación.

b. Control de errores

b.1 Causas

Como se conoce, los medios de transmisión de datos introducen errores que pueden ser influenciados por las siguientes razones:

- Distancia entre emisor y receptor de datos
- Número de repetidores sobre el medio de transmisión
- Soporte de transmisión

- Ritmo de transmisión
- Tipo de codificación y/o modulación
- Interferencias causadas por ruido, atenuación y otros.

Las técnicas de control de errores varían según los tipos de errores que son más comunes en cada sistema.

b.2 Métodos de control de errores

Los métodos de control de errores más comunes son:

1. Eco (repetición de datos recibidos)
2. Códigos de paridad y bloque
    - Paridad horizontal
    - Paridad vertical
    - Código de Hamming (de corrección de error)
    - Transmisión entrelazada
3. Códigos basados en división módulo 2
    - Código de redundancia cíclica (CRC)
    - Código de Fire (corrección de grupos de errores)
4. Códigos de convolución

b.3 Estrategias de corrección de errores

Una vez que se detecta el error, existen varias estrategias de corrección:

- Espera de confirmación o reconocimiento (ACK) de cada bloque antes de enviar otro. Ej: BSC
- Transmitir n bloques, esperar confirmación, retransmitir el bloque errado y todos los que le siguen. Ej: HDLC
- Repetición selectiva. Sólo se retransmite el bloque errado.
- Corrección sin repetición. El receptor corrige eventuales errores de transmisión. Ej: Código de convolución o de fire.

b.4 Clases de códigos de detección y corrección de errores

Se conocen básicamente dos clases grandes de códigos:

1. Códigos de bloque
2. Códigos convolucionales

1. Códigos de bloque. En un código bloque un número fijo k de símbolos de información son transformados en una secuencia de n $(n > k)$ símbolos código a ser transmitidos al receptor. La característica de un código bloque (contraria a un convolucional) es que los n símbolos código de un bloque dado dependen solamente de un conjunto particular de k símbolos de información.

2. Códigos de convolución. En los códigos de convolución o recurrentes, la codificación y decodificación se hace en diferido y se lo utiliza cuando la transmisión de datos no se realiza en tiempo real o cuando los errores se producen en paquetes. La capacidad de corrección automática es grande y se utiliza en transmisión de datos por satélite. A diferencia de los códigos bloque, los códigos convolucionales no permiten la división de los símbolos de información en bloques, en este caso los bits son codificados según el valor de los k bits anteriores y m bits posteriores.

c. Control de secuencias de paquetes

El control de secuencia de paquetes se utiliza para ordenar los paquetes en la secuencia adecuada y de esta forma reconstruir los mensajes del nivel superior. Como se verá posteriormente, este tipo de control se utiliza a nivel de la capa de red, donde se utilizan los datagramas, paquetes que normalmente llegan desordenados. Sin embargo, también puede ser necesario con redes de circuitos virtuales grandes.

Los errores al utilizar este control, podrían presentarse cuando falla un enlace y se lo configura nuevamente, empezando de esta forma a retransmitir tramas. De esta forma, los paquetes demorados del primer enlace podrían llegar después de los paquetes numerados de forma similar en el segundo enlace.

Aunque las implementaciones del control de secuencias de paquetes se las hace frecuentemente en el nivel red, también se utilizan en el nivel transporte.

Técnicas de control de servicios en el subnivel LLC

De los servicios de conexión expuestos, el subnivel enlace de datos LLC proporciona los servicios orientados a conexión sin implementar el secuenciamiento de paquetes. Es decir, el subnivel enlace de datos LLC proporciona los siguientes servicios mediante los reconocimientos:

1. Control de flujo a nivel LLC
2. Control de errores

1. Control de flujo al nivel de LLC. El control de flujo al nivel de LLC permite retardar a los dispositivos más rápidos para que puedan comunicarse con los más lentos. El control de flujo a nivel en enlace de datos utiliza los reconocimientos para controlar el flujo de datos en función de las capacidades del dispositivo. Podría decirse que el control de flujo a este nivel se hace en el segmento de red, no en la internet.

2. Control de errores al nivel de LLC. El control de errores a este nivel (subnivel LLC) se refiere a la notificación de paquetes perdidos o mezclados. Los dos estados de control de errores en el subnivel LLC son:

    - Si el receptor previsto no recibe un paquete, el dispositivo transmisor no recibe un reconocimiento ó el que recibe es un reconocimiento negativo (NACK), el transmisor asume que existió un error en la transmisión.
    - Si las sumas de comprobación no coinciden, es decir, si el receptor capturó una trama de entrada, pero la suma de comprobación no coincide con la que le proporcionó el transmisor se concluirá que existió un error y el receptor podrá pedir una retransmisión.

1.2.5.3 El nivel red OSI

Las unidades de datos en este nivel son conocidas como paquetes. El propósito básico del nivel red es permitir el direccionamiento de datos a un nivel más alto que el de la capa enlace de datos. Es decir, mientras en la capa enlace de datos se tenía un direccionamiento físico (utilizando las direcciones MAC de los equipos que se conectaban en un mismo segmento de red), la capa red proporciona un direccionamiento lógico (utilizando direcciones de red lógica y servicio, incluso entre diferentes segmentos de red).

Las principales funciones de las que es responsable el nivel red son:

- Seleccionar el mejor camino a través de una internet[6].
- Evitar el envío de datos a redes que no tengan relación, disminuyendo de esta manera el tráfico en las redes. Esto lo consigue mediante técnicas de direccionamiento y conmutación utilizando algoritmos de asignación de ruta.
- Garantizar rutas correctas para los datos a través de una internet o de redes distintas.

Las técnicas utilizadas en el nivel red son aplicables por las siguientes razones:

- Todas las redes lógicamente diferentes deben tener direcciones de red únicas.
- Las conexiones en la internet requieren que se realice un proceso de conmutación.
- La necesidad de elegir el mejor recorrido ha determinado que se implementen técnicas de asignación de ruta.
- La necesidad de disminuir la cantidad de errores previstos en la red requiere que se implementen distintos niveles de servicios de conexión.

[6] Se utilizará el término internet en adelante, para referirnos a una red formada por varios segmentos que requieran de funciones de la capa red para comunicarse. No confundir con el término Internet utilizado para hacer referencia a la gran red mundial. Recordemos que esta tesis es orientada a redes de área local.

Para ser verdaderamente prácticos, una internet debe representar consistentemente las rutas de sus conexiones al medio. En la siguiente figura cada línea entre los ruteadores tiene un número que los ruteadores usan como dirección de red. Estas direcciones deben cubrir información que pueda ser usada por un proceso de enrutamiento.

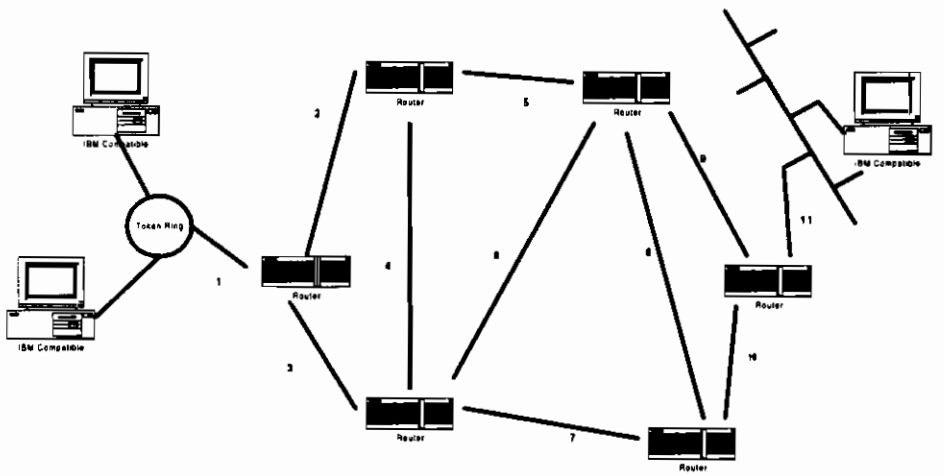


***Figura 1.30* Enrutamiento de datos**

Esto significa que una dirección debe tener información sobre la ruta de las conexiones del medio usadas por el proceso de enrutamiento para pasar paquetes desde una fuente hacia un destino.

La capa de red combina esta información (de la ruta de las conexiones en los enlaces) dentro de una internet, añadiendo la determinación de la ruta, conmutación de ruta, y funciones de procesamiento de ruta a un sistema de comunicaciones. Usando estas direcciones, la capa red también provee una manera de interconectar redes independientes.

La consistencia de las direcciones de la capa red que cruzan toda la internet, también mejoran el uso de ancho de banda al prevenir el uso de *broadcast* innecesario.

A. *Hardware* de conectividad de red asociado con el nivel red OSI

Al nivel red del modelo OSI está asociado el siguiente *hardware* de conectividad:

1. Ruteadores:

   Función: Conectar dos o más redes separadas lógicamente. A las separaciones lógicas se las suele denominar subredes. Las funciones de los ruteadores y *bridges* son semejantes, pero los ruteadores realizan selección de recorridos más sofisticados con actividades de

procesamiento intensas, razón por la cual las velocidades de procesamiento de paquetes no son tan altas como en los *bridges*.

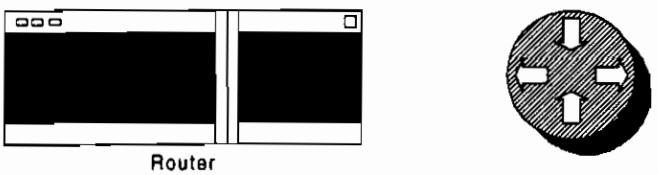


***Figura 1.31** Ruteador y su representación típica*

2. *Brouters*:

Función : Son esencialmente routers que también realizan funciones de *bridges*. Los *Brouters* primero comprueban si admiten el protocolo que utiliza el paquete, sino es así, en lugar de dejar caer el paquete, utilizan la información de la dirección física para direccionarlo.

B. Temas y técnicas del nivel red OSI

Nivel OSI	Temas	Técnicas
Red	Direccionamiento	Red lógica Servicio
	Conmutación	Paquete Mensaje Circuito
	Descubrimiento de ruta	Vector de distancia Estado de enlace
	Selección de ruta	Estático Dinámico
	Servicios de conexión	Control de flujo al nivel red Control de errores Control de secuencia de paquetes
	Servicios de *gateway*	Traducción de nivel red

***Tabla 1.15** Temas y técnicas del nivel red OSI*

B.1 Direccionamiento

De manera general se conocen tres tipos de direccionamiento:

1. Utilizando las direcciones MAC (usado por el nivel enlace de datos).
2. Utilizando direcciones de red lógica (usado por el nivel red)
3. Utilizando direcciones de servicios (usado por nivel red)

La figura 1.32 muestra la forma en que se relacionan estos tipos de direccionamiento:

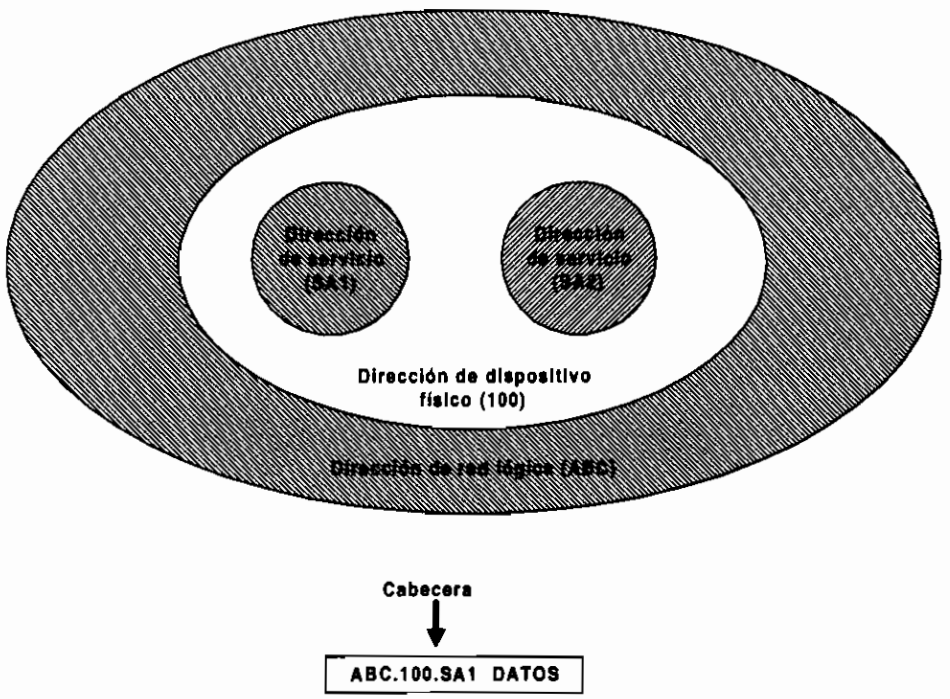


Figura 1.32 Tipos de direcciones de una red de datos

Debido a que el direccionamiento utilizando las direcciones MAC fue revisado en la parte correspondiente a "Técnica de dispositivo físico (Direcciones MAC)" en el nivel enlace de datos, corresponde en esta parte hacer referencia a las técnicas de direccionamiento utilizadas en el nivel red.

B.1.a Técnica de direccionamiento utilizando direcciones de red lógica

A diferencia del direccionamiento usando direcciones MAC (direcciones preestablecidas y usualmente relacionadas a un dispositivo), una dirección de red tiene una relación lógica.

Para algunos protocolos de la capa red[7], esta relación es establecida por un administrador de red quien asigna las direcciones de red de acuerdo a algún plan de direccionamiento de internet preconcebido. Para otros protocolos de la capa red, la asignación de direcciones es parcial o totalmente dinámica.

Las direcciones de dispositivo físico sólo identifican loas dispositivos de una única red. Para la entrega de datos en una internet se deben utilizar direcciones de red lógicas.

[7] Es importante que se diferencie entre *protocolo de ruta y protocolo de enrutamiento*. El protocolo de ruta es usado entre ruteadores para dirigir el tráfico de usuario (ej. IP, IPX). El protocolo de enrutamiento es usado solamente entre ruteadores para mantener tablas de ruta (ej. RIP, IGRP).

Cuando se establece una red LAN o WAN, es importante garantizar que la dirección de cada red sea exclusiva.

B.1.b Técnica de direccionamiento utilizando direcciones de servicios

Las direcciones de dispositivo físico (MAC) en conjunto con las direcciones lógicas, pueden utilizarse para el traslado de datos en una internet. Sin embargo, cada dispositivo de red puede representar varios papeles simultáneamente (el término entidad identifica el *hardware* y *software* que representa cada papel individual).

Cada entidad debe tener su propia dirección de tal forma que puedan enviar y recibir datos. A esta dirección se la denomina dirección de servicio (en algunos protocolos se la denomina dirección de puerto o zócalo). Se pueden asignar varias direcciones de servicio a un dispositivo que está ejecutando varias aplicaciones de red (es decir que representa a varias entidades).

Cuando dos entidades desean comunicarse, anexan direcciones de servicio a las direcciones lógicas y de dispositivos físicos:

- La dirección lógica indica la red de origen o destino.
- La dirección de dispositivo físico (MAC) identifica el computador de origen o destino.
- La dirección de servicio se refiere al proceso de aplicación específico que se está ejecutando en el dispositivo de origen o destino.

B.2 Conmutación

Debido a que en internets de gran tamaño los caminos factibles para conectar dos puntos (origen y destino) pueden ser muchos, es necesario utilizar técnicas de conmutación que permitan que la información se pueda conmutar a medida que viaja a través de los distintos canales de comunicación. A continuación se numeran las técnicas de conmutación conocidas:

- Conmutación de circuitos
- Conmutación de mensajes
- Conmutación de paquetes

Técnicas de conmutación del nivel red

a. Conmutación de circuitos

Esta técnica se encarga de conectar al emisor y receptor mediante un único camino durante el intervalo de la conversación.

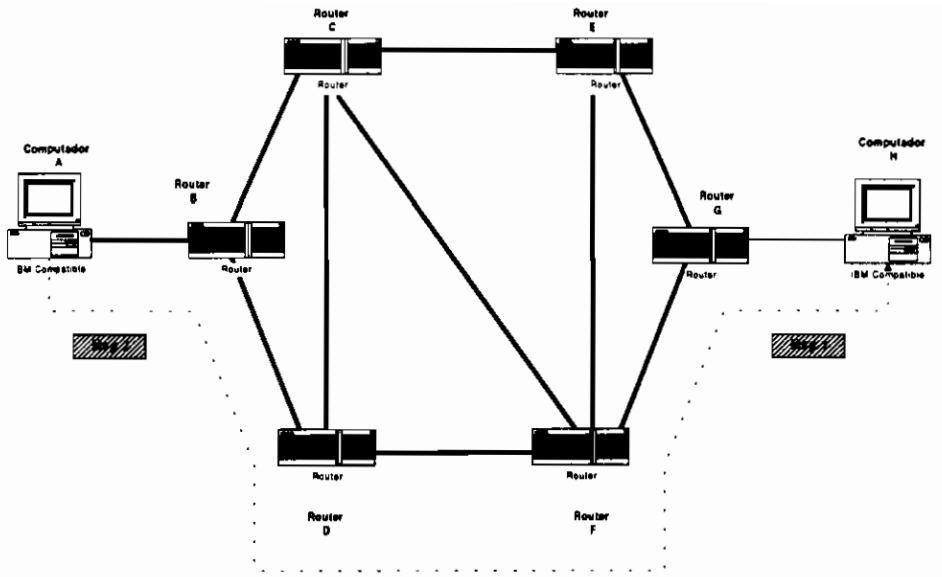


***Figura 1.33** Transmisión de datos utilizando conmutación de circuitos*

Antes de que se pueda tener acceso a la comunicación entre los extremos, debe estar trazado el recorrido completo. La computadora que inicia la transferencia de datos debe solicitar una conexión con la de destino. Una vez establecida la conexión con este tipo de técnica de conmutación, existe un recorrido dedicado entre los dos extremos hasta que se interrumpa la conexión. Esta técnica de conmutación es semejante a la que se utiliza en las centrales telefónicas cuando dos abonados establecen comunicación.

Ventajas	Inconvenientes
Canal de datos dedicado con velocidad de datos garantizada	Único canal hace ineficaz el uso del medio
Virtualmente no existen demoras en el acceso al canal después de haber establecido el circuito	Los canales dedicados son relativamente costosos en tiempo, dinero y ancho de banda.
	Está sujeto a largas demoras de conexión.

***Tabla 1.16** Ventajas e inconvenientes de la conmutación de circuitos como técnica de conmutación del nivel red*

b. Conmutación de mensajes

La conmutación de mensajes no establece un recorrido dedicado entre origen y destino mientras dura la conversación. Las conversaciones se dividen en mensajes. Cada mensaje se empaqueta con su propia dirección de destino y se transmite a través de la red. Los dispositivos intermedios reciben el mensaje, lo almacenan temporalmente y a continuación los

transmiten al siguiente dispositivo. Este tipo de técnica se la conoce como almacenar y enviar (*store and forward*).

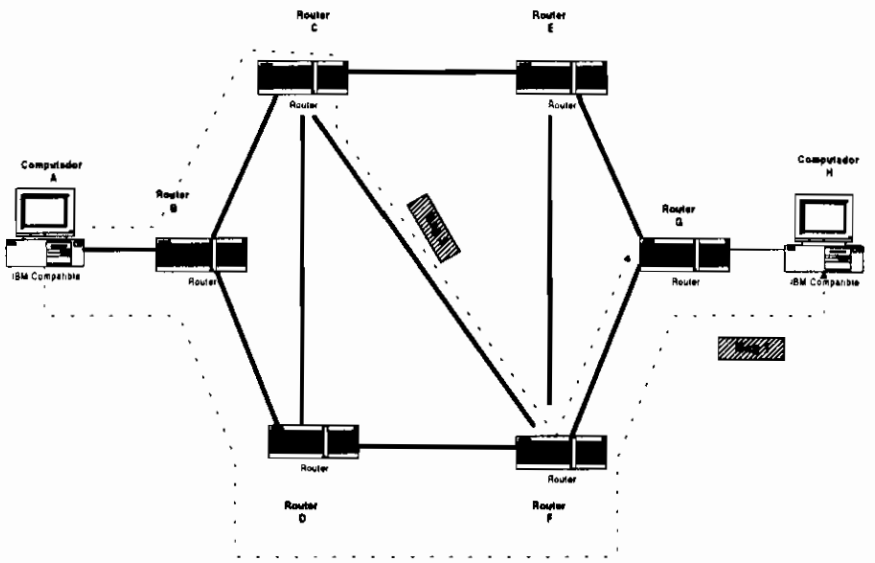


***Figura 1.34** Transmisión de datos utilizando conmutación de mensajes*

Ventajas	Inconvenientes
El ancho de banda lo pueden compartir varios dispositivos, de tal forma que es mejor aprovechado que en la conmutación de circuitos.	No es útil en la mayoría de aplicaciones de tiempo real como en comunicaciones de audio y video.
El almacenamiento temporal reduce el tráfico de la red.	Puede resultar costoso debido a los dispositivos que se encargan del almacenamiento y envío, especialmente por la capacidad de almacenamiento que deberán tener reservada para mensajes potencialmente largos.
Se puede dar niveles de prioridad a los mensajes, de forma que los mensajes con baja prioridad se puedan demorar.	
Se pueden utilizar direcciones de difusión para enviar mensajes a múltiples destinos.	
Se mejoran las comunicaciones globales (en distintas zonas horarias) pues no es necesario que el receptor esté presente cuando se envía el mensaje.	

***Tabla 1.17** Ventajas e inconvenientes de la conmutación de mensajes*

La técnica de almacenar y enviar requiere de dispositivos de conmutación de mensajes que tengan suficiente capacidad de almacenamiento como para retener temporalmente los mensajes de entrada, que podrían ser largos. Está por tanto incluida una demora debido al tiempo requerido para encontrar la siguiente parada del mensaje, guardarlo y volverlo a enviar hasta que llegue a su destino final.

Aplicaciones:

La conmutación de mensajes se suele utilizar en servicios como correo electrónico, agendas, flujo de trabajo y trabajo en grupo.

c. Conmutación de paquetes

Esta técnica combina las ventajas de la conmutación de circuitos y mensajes y reduce las desventajas de ambas. Se tratan dos métodos de conmutación de paquetes:

- Conmutación de paquetes de datagramas
- Conmutación de paquetes de circuitos virtuales

En los dos métodos de conmutación de paquetes, los mensajes se dividen en pequeñas partes, denominadas paquetes. Cada paquete se marca con direcciones de origen, paso intermedio y destino. Los paquetes tienen definida una longitud máxima y se pueden almacenar en memoria temporal de acceso más rápido (como en las RAM), en lugar de discos duros (lo que mejora el tiempo de acceso y reduce los requisitos de *hardware* para el almacenamiento).

c.1 Conmutación de paquetes de datagramas

La conmutación de paquetes de datagramas es semejante a la conmutación de mensajes, en ambos casos la información se divide en unidades más pequeñas para ser transmitida. La diferencia es que en el datagrama a más de añadir información de direccionamiento (como en la conmutación de mensajes) se añade un número de secuencia a cada paquete, debido a que los paquetes pueden llegar desordenados a su destino.

Los datagramas se envían por la ruta que en su momento cada dispositivo decide que es la más apropiada para cada paquete. El dispositivo receptor finalmente recibe los paquetes (datagramas), los ordena por su número de secuencia y reconstruye el mensaje original. La técnica de secuenciamiento de paquetes fue tratada en el tema de servicios de conexión del nivel enlace de datos, y será revisada en el mismo tema en esta sección.

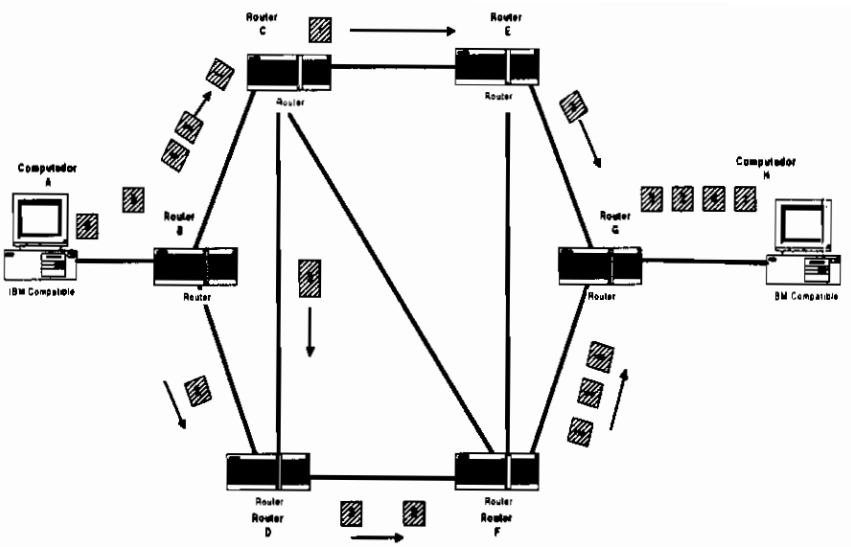


Figura 1.35 Transmisión de datos utilizando conmutación de paquetes

Aplicaciones: La conmutación de paquetes de datagramas se utiliza con topologías físicas de LAN multipunto.

c.2 Conmutación de paquetes de circuitos virtuales

Los circuitos virtuales son conexiones lógicas entre el emisor y el receptor. Cuando el emisor y receptor intercambian mensajes durante la conversación, estos mensajes permiten establecer acuerdos respecto a tamaño máximo de mensajes, recorrido a escoger y otras variables con el fin de establecer y mantener la conversación, obteniendo de esta forma una conexión lógica.

Ventajas	Inconvenientes
Los dispositivos no requieren unidades de gran almacenamiento como en la conmutación de paquetes de datagramas.	Involucra tecnología y protocolos más complejos y por tanto costos más altos
Existen menos demoras en las transmisiones	Requieren mayor cantidad de retransmisiones porque los paquetes se pierden más fácilmente.
Los paquetes se manejan bien aún en enlaces problemáticos	
Utilización óptima del ancho de banda	

Tabla 1.18 Ventajas e inconvenientes de la conmutación de paquetes como técnica de conmutación del nivel red

Los circuitos virtuales generalmente implican servicios de conexión orientados a conexión (control de errores, control de flujo y secuenciamiento de paquetes mediante reconocimientos). Los circuitos temporales pueden ser de dos tipos:

- Temporales (cuando duran exclusivamente el tiempo de conversación)
- Permanentes (cuando duran mientras el dispositivo origen y destino estén funcionando).

Aplicaciones: Es utilizado en enlaces problemáticos.

Diferenciación entre protocolos de descubrimiento de ruta y protocolos de selección o asignación de ruta

Antes de continuar con los temas correspondientes a descubrimiento de ruta y selección (o asignación) de ruta, es importante que se tengan claros los conceptos de protocolos de descubrimiento de ruta (o protocolos de enrutamiento) y protocolos de selección o asignación de ruta (o protocolos de ruteo).

Los protocolos de enrutamiento (conocidos en inglés también como *routing protocols*) son los protocolos utilizados solamente entre ruteadores para mantener tablas de enrutamiento o ruteo. Los protocolos de enrutamiento soportan un protocolo de ruteo (o de selección de ruta) proveyendo de mecanismos para compartir información de enrutamiento. Los mensajes de los protocolos de enrutamiento se mueven entre los ruteadores. Un protocolo de enrutamiento permite a los ruteadores comunicarse unos con otros, para actualizar y mantener las tablas de ruteo. Los protocolos de enrutamiento no llevan tráfico de usuario final de red a red. Un protocolo de enrutamiento usa los protocolos de ruteo para pasar información entre ruteadores. Ejemplos de protocolos de enrutamiento (o de descubrimiento de ruta) son: RIP, OSPF, IGRP.

Los protocolos de ruteo (conocidos en inglés también como *routed protocols*) son los protocolos usados entre ruteadores para direccionar el tráfico de usuario. Cualquier *stack* de protocolos[8] que provea suficiente información en su dirección de capa red puede permitir direccionar los paquetes de tráfico de usuario. Los protocolos de ruteo (o selección de ruta) definen el formato y el uso de los campos dentro de un paquete. Los paquetes generalmente son llevados desde un sistema final a otro. Ejemplos de protocolos de ruteo (o de selección o asignación de ruta) son: IP, IPX.

B.3 Descubrimiento de ruta

Para que cada uno de los paquetes llegue a su dispositivo destino, debe identificarse el mejor camino o ruta por el que cada parte de los datos tiene que viajar.

[8] Un *stack* de protocolos hace referencia a una serie ordenada en una jerarquía lógica de protocolos.

Antes de que una entidad de red pueda empezar a asignar (seleccionar) una ruta, debe descubrir la ruta que debería tomar un paquete para llegar al destino previsto.

De esta forma, se podría describir el descubrimiento de ruta como el proceso que se utiliza para identificar rutas y mantener tablas de ruta. Las tablas de ruta indican el siguiente salto al que se dirigen los paquetes para llegar al destino. Las tablas de ruta incluyen direcciones de red, la siguiente dirección del recorrido de los datos y el costo para alcanzar el destino.

El costo se calcula usando algoritmos de asignación de ruta y pueden establecerse de acuerdo a lo siguiente:

- El recuento de saltos: es el número de ruteadores por los que se debe pasar antes de llegar a la red destino.
- El recuento de pulsaciones: es la cantidad de tiempo necesaria para llegar a la red destino.
- El gasto relativo: es un número que se asigna considerando criterios necesarios para asignación de una ruta específica. Estas asignaciones se utilizan por ejemplo cuando se quiere disminuir el uso de un canal de costo elevado.

Para hacer una analogía, así como las redes de computadores deben identificar la ubicación de las direcciones del nivel red y determinar las rutas para la entrega de paquetes, los carteros deben identificar la ubicación de las direcciones de su zona antes de entregar el correo. Una vez que se han identificado varias direcciones, el cartero asigna una ruta lógica para entregar las cartas.

La mayoría de algoritmos de ruteo o técnicas de ruteo pueden ser clasificados de acuerdo a uno de dos algoritmos básicos:

- Vector de distancia
- Estado de enlace

Una tercera clasificación llamada híbrida combina aspectos de los dos algoritmos básicos.

No hay un único algoritmo de ruteo para todas las internetes. Los administradores de red deben medir aspectos técnicos y no técnicos de sus redes para determinar cual es mejor.

B.3.a Tiempo de convergencia

Antes de continuar con las técnicas de descubrimiento de ruta, es conveniente que se tenga conocimiento sobre el problema de tiempo de convergencia que se resume a continuación:

- La convergencia ocurre cuando todos los ruteadores usan una perspectiva consistente de la topología de red.
- Después de un cambio en la topología, los ruteadores deben recalcular las rutas.
- El proceso y tiempo requerido para la reconvergencia del ruteador varía de acuerdo a los protocolos de enrutamiento.

El algoritmo de enrutamiento es fundamental para el ruteo dinámico (que será visto posteriormente). Cuando la topología de una red cambia debido al crecimiento, reconfiguración o falla, la base del conocimiento de la internet también debe cambiar.

La base del conocimiento necesita reflejar una visión exacta y consistente de la nueva topología. Esta visión exacta y consistente es llamada convergencia. Cuando todos los ruteadores en una internet están operando con la misma base conocida, se dice que la internet es convergente.

La convergencia rápida es una característica deseable de internet, debido a que aquella reduce el periodo de tiempo que los ruteadores permanecen con una base de conocimiento desigual, lo que podría producir que se tomen decisiones de enrutamiento que podrían ser incorrectas o desperdiciadas.

B.3.b Técnicas de descubrimiento de ruta

a. Vector de distancia

Los algoritmos de enrutamiento de vector de distancia (también conocidos como algoritmos *Bellman-Ford*) pasan copias periódicas de una tabla de enrutamiento desde un ruteador a otro. Las actualizaciones regulares entre ruteadores comunican los cambios de topología.

Cada ruteador recibe una tabla de ruteo desde su "vecino" más cercano (ruteador que se encuentra en el mismo segmento de red). Por ejemplo en la figura, el ruteador B recibe información del ruteador A. El ruteador B añade un número de vector de distancia (como un número de saltos) incrementando el vector de distancia y pasa la tabla de enrutamiento a su otro ruteador más próximo, el ruteador C. Este mismo proceso ocurre paso a paso en todas las direcciones entre los ruteadores directamente próximos.

De esta forma, el algoritmo acumula distancias de red, permitiendo mantener una base de datos de información de la topología de la internet. Sin embargo, debido a que la internet en algunos casos podría ser grande y compleja, y debido a que cada dispositivo sólo obtiene información actualizada de sus vecinos cuando ellos han asimilado la actualización, el método de vector de distancia puede necesitar una cantidad relativamente grande de tiempo para cambiar todas las tablas de direcciones de la red.

Eventualmente los ruteadores se darán cuenta de los cambios, pero las tablas de rutas completas, incluyendo los cambios, deben pasar de un ruteador a otro.

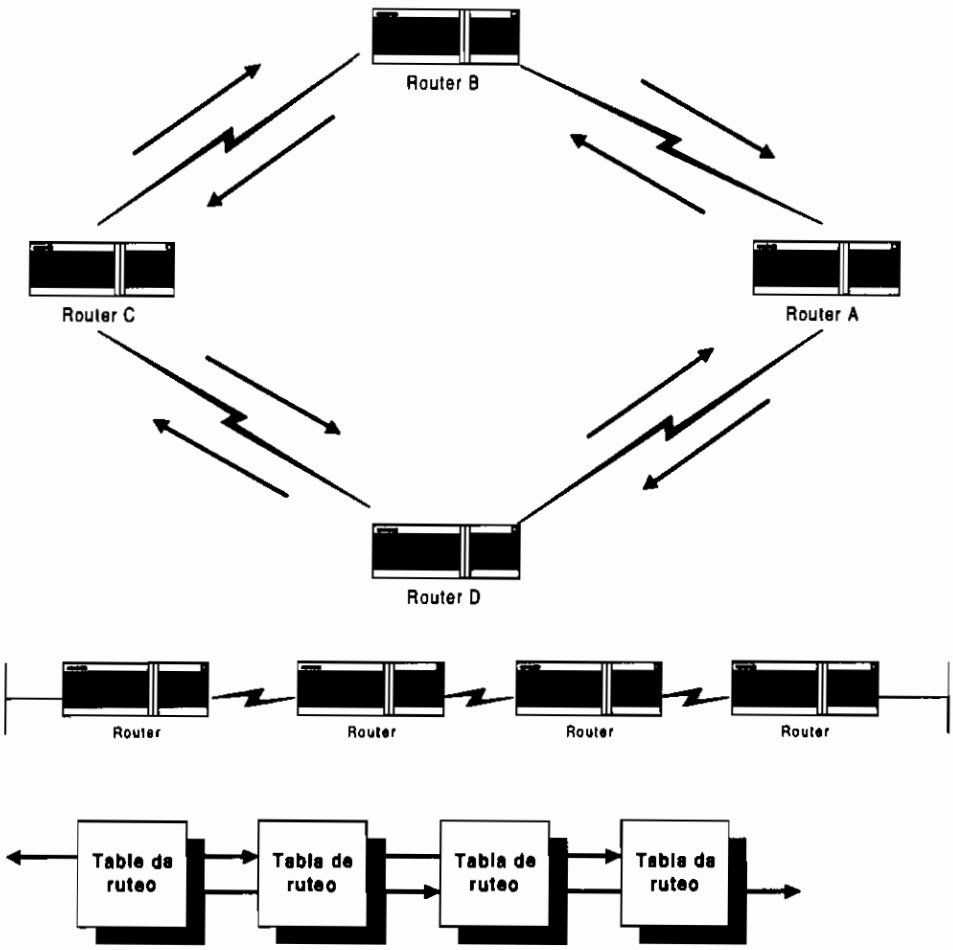


Figura 1.36 Descubrimiento de ruta utilizando vector de distancia

Cuando se utiliza el método de vector de distancia, se recoge información de costos incrementando la información de saltos, pulsaciones o gastos relativos de otras tablas.

a.1 Descubrimiento de la red utilizando vector de distancia

Cada ruteador que utiliza enrutamiento de vector de distancia comienza por identificar sus propios vecinos. En la figura 1.37, el pórtico conectado directamente a cada red es mostrado como una distancia 0.

Debido al funcionamiento del proceso de descubrimiento de ruta con vector de distancia, los ruteadores descubren el mejor camino a las redes destino basadas en las medidas acumuladas desde cada ruteador vecino.

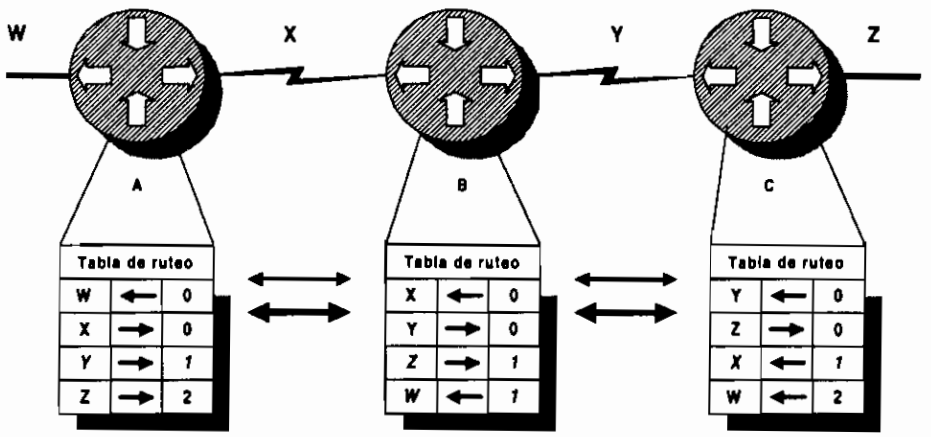


Figura 1.37 Descubrimiento de ruta utilizando vector de distancia en sus tablas de ruteo

Por ejemplo, el ruteador A aprende sobre otras redes no contiguas basadas en la información que recibe del ruteador B. Cada una de estas entradas de red en la tabla de ruteo tienen un vector de distancia acumulado que muestra cuan lejos de esa red se encuentra en la dirección dada.

a.2 Actualización ante cambios de topología usando vector de distancia

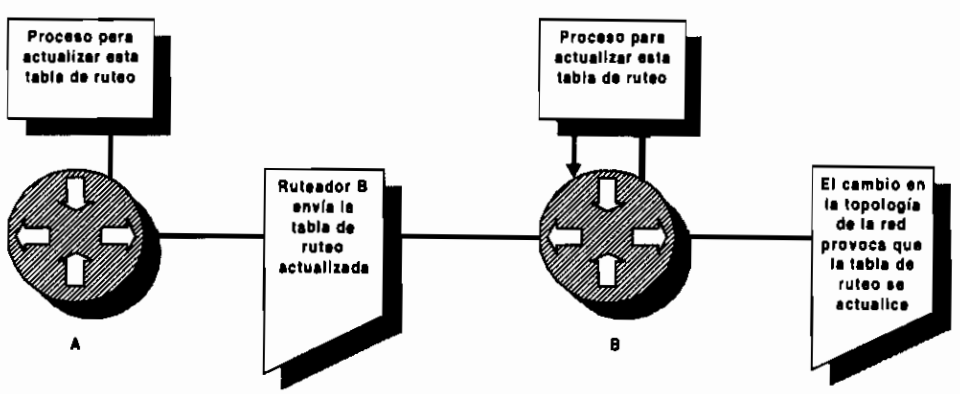


Figura 1.38 Proceso de actualización de las tablas de ruta cuando se utiliza vector de distancia en el descubrimiento de ruta

Cuando cambia la topología en una red donde se utilizan protocolos con descubrimiento de ruta de vector de distancia, debe ocurrir la actualización de tablas de ruteo. Como con el proceso de descubrimiento de red, el proceso de actualización del cambio de topología ocurre paso a paso desde ruteador a ruteador.

Los algoritmos de vector de distancia llaman a cada ruteador próximo para enviarle la tabla de ruteo. Las tablas de ruteo de vector de distancia incluyen información acerca del costo total de la ruta (definida por su

métrica[9]) y la dirección del primer ruteador sobre la ruta a cada red sobre la que tiene conocimiento.

Cuando un ruteador recibe una actualización de un ruteador próximo, compara la tabla recibida con la que tenía inicialmente. Si puede aprender desde su vecino de una mejor ruta (métrica más pequeña) a una red, el ruteador actualiza su tabla de ruteo inicial. Una vez actualizada, el ruteador añade el costo de alcanzar el ruteador más próximo al costo de la ruta reportada por su vecino para establecer la nueva métrica.

Por ejemplo, si el ruteador A en la figura 1.38 tiene una unidad del costo desde el ruteador B, el ruteador A debería añadir 1 a todos los costos reportados por el ruteador B cuando aquel corre el proceso de vector de distancia para actualizar su tabla de ruteo.

Problema: Lazos de enrutamiento (*Routing loops*)

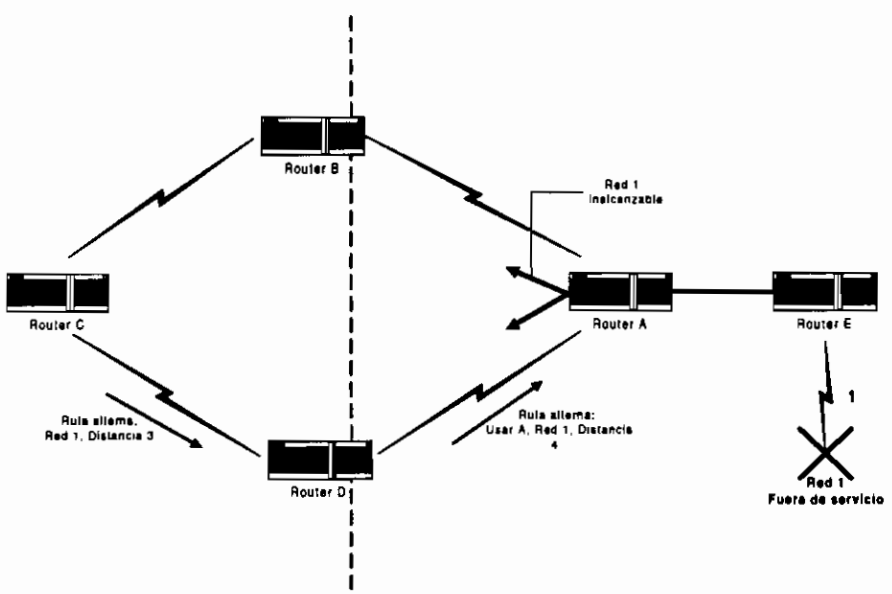


***Figura 1.39* Problema de lazos de enrutamiento al utilizar la técnica de vector de distancia en el descubrimiento de ruta**

Los lazos de enrutamiento pueden ocurrir si la convergencia de la internet es baja debido a una nueva configuración que causa entradas de ruteo inconsistentes. La figura 1.39 ilustra como un lazo de enrutamiento puede ocurrir:

[9] Una métrica es una cualidad asignada a un determinado enlace. Al valor asignado a esa cualidad para cuantificar la facilidad o dificultad de transmitir a través de un enlace determinado, se lo conoce como valor de la métrica. Normalmente un valor bajo de métrica indica que el enlace o ruta es fácilmente alcanzable.

- Antes de la falla en la red 1, todos los ruteadores tienen conocimiento consistente y tablas de ruteo correctas, es decir se habla de una red convergente. Asumamos para resumir este ejemplo, que la ruta preferida del ruteador C a la red 1 es por medio del ruteador B, y que el ruteador C tiene una distancia de 3 a la red 1 en su tabla de ruteo.
- Cuando la red 1 falla, el ruteador E envía una actualización al ruteador A. El ruteador A detiene los paquetes enrutados a la red 1, pero los ruteadores B, C, y D continúan haciéndolo, debido a que ellos todavía no han sido informados sobre la falla. Cuando el ruteador A envía su actualización, los ruteadores B y D paran el ruteo a la red 1; sin embargo, el ruteador C todavía no está actualizado. Para el ruteador C, la red 1 es todavía alcanzable por medio del ruteador B.
- Ahora el ruteador C envía una actualización periódica al ruteador D indicando una ruta a la red 1 por medio del ruteador B. El ruteador D cambia su tabla de ruteo actualizando el nuevo camino erróneo, y propaga esta información al ruteador A. El ruteador A propaga esta información al ruteador B y E, y así sucesivamente. De esta forma, cualquier paquete destinado a la red 1 entrará en un lazo que va desde el ruteador C al B al A al D y regresa a C.

Problema: Cuenta al infinito

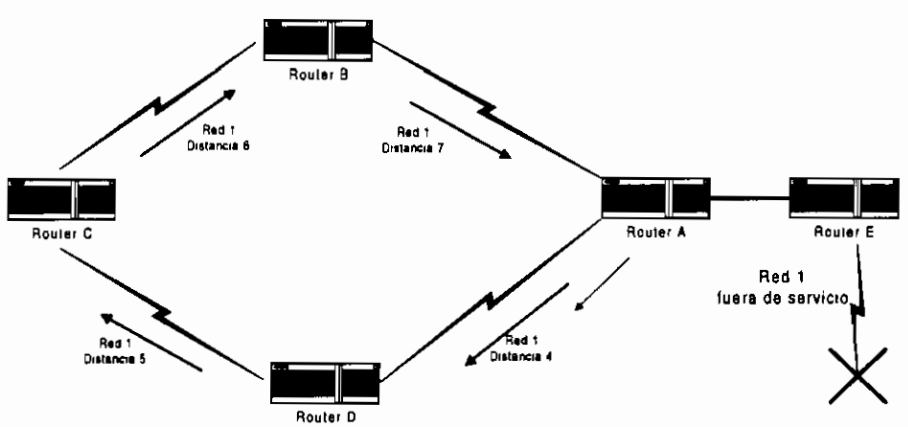


Figura 1.40 Problema de cuenta al infinito al utilizar la técnica de vector de distancia en el descubrimiento de ruta

Continuando con el ejemplo anterior, la actualización inválida respecto a la red 1 continúa en lazo. Hasta que algún otro proceso pueda parar el lazo, los ruteadores actualizan sus tablas con una vía inapropiada considerando que la red 1 está aún fallando.

Esta condición, llamada cuenta al infinito, continuamente pone en lazo a paquetes alrededor de la red, considerando que la red 1 destino está fallida. Mientras las ruteadores estén contando al infinito, la información inválida permite que exista el lazo de enrutamiento. Con un vector de

distancia de cuenta de salto, el vector incrementa cada vez que pasa a través de otro ruteador.

Solución: Definiendo un máximo

Los algoritmos de enrutamiento de vector de distancia son auto corregibles, pero el problema de lazo de enrutamiento puede requerir que una cuenta al infinito suceda primero.

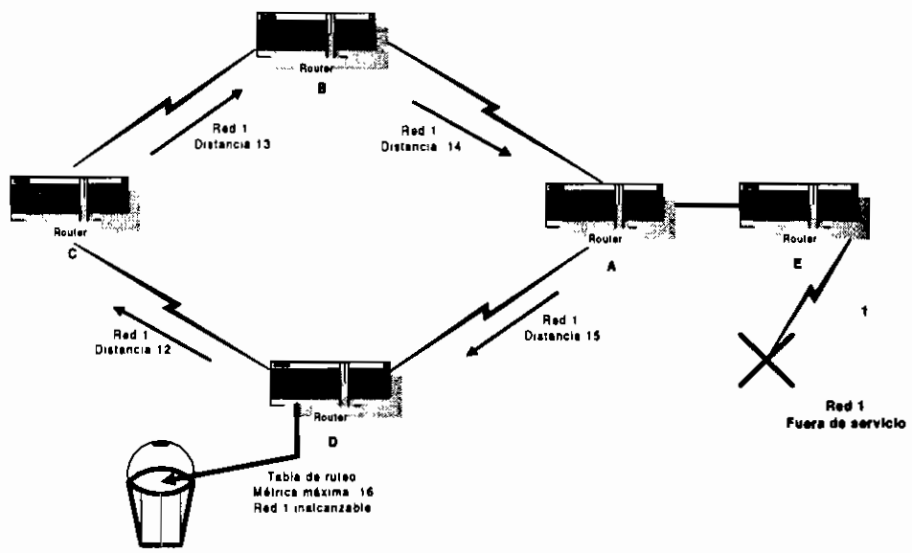


Figura 1.41 Definición de un máximo como solución al problema de cuenta al infinito al utilizar la técnica de vector de distancia en el descubrimiento de ruta

Para evitar este problema prolongado, los protocolos de vector de distancia definen un infinito como algún número máximo. Este número se refiere a una métrica de enrutamiento (por ejemplo, un simple conteo de salto).

Con esta aproximación, el protocolo de enrutamiento permite que el lazo de enrutamiento exista hasta que la métrica exceda su valor máximo permitido. La figura 1.41muestra este máximo definido a 16 saltos; para vectores de distancia de conteo de saltos, un número de 15 saltos es comúnmente usado. En cualquier caso, una vez que el valor de la métrica excede el máximo, la red 1 es considerada inalcanzable.

Solución: Split Horizon

Otra fuente posible para que el lazo de enrutamiento ocurra es que información incorrecta sea enviada de regreso a un ruteador contradiciendo la información que envió. Así es como este problema ocurre:

- El ruteador A pasa una actualización al ruteador B y ruteador D indicando que la red 1 está fallando. Sin embargo, el ruteador C transmite una actualización al ruteador B indicando que la red 1 es disponible con una distancia de 4 por medio del ruteador D.
- El ruteador B concluye (incorrectamente) que el ruteador C todavía tiene un camino válido a la red 1, si bien con una métrica mucho menos favorable. El ruteador B envía una actualización al ruteador A advirtiendo de un nuevo camino hacia la red 1.
- El ruteador A ahora determina que puede hacer envíos a la red 1 por medio del ruteador B; el ruteador B determina que puede hacer envíos a la red 1 a través del ruteador C; y el ruteador C concluye que puede hacer envíos a la red por medio del ruteador D. Cualquier paquete introducido dentro de este medio quedará en lazo dentro de los ruteadores.

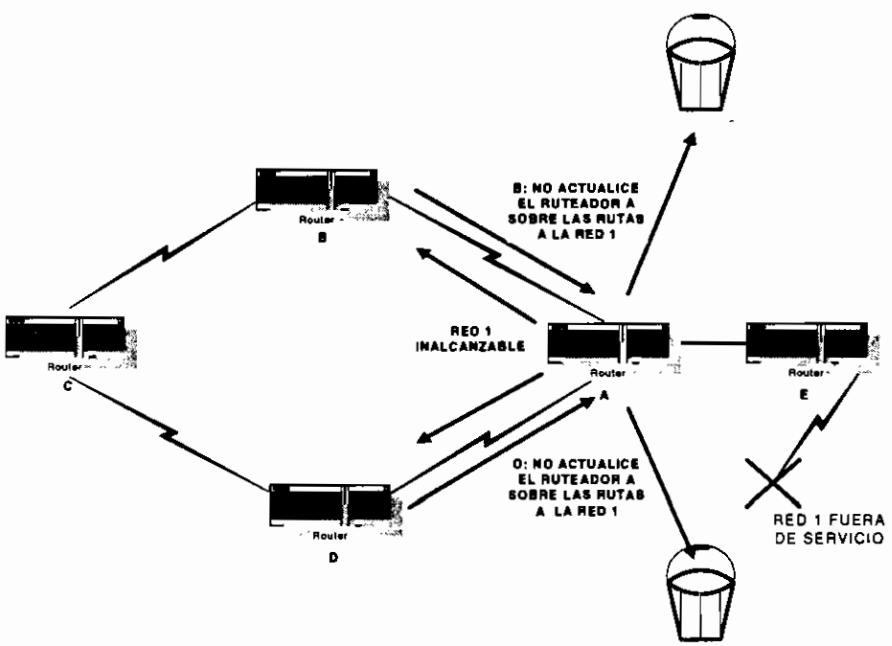


***Figura 1.42** Utilización de split horizont para solucionar el problema de lazos de enrutamiento al utilizar la técnica de vector de distancia en el descubrimiento de ruta*

Split Horizon evita esta situación. Como se muestra en la figura 1.42, si una tabla actual sobre la red 1 llega desde el ruteador A, el ruteador B o D no pueden enviar información sobre la red 1 de regreso al ruteador A. Split Horizon reduce de esta manera la información de enrutamiento incorrecta y reduce la sobrecarga (tráfico) en la red.

Solución: Envenenamiento de ruta (*Route poisoning*)

El envenenamiento de ruta es otra técnica para que los ruteadores eviten problemas causados por actualizaciones inconsistentes. Con esta técnica, el ruteador configura una entrada de tabla que guarda el estado de red

consistente mientras otros ruteadores gradualmente convergen correctamente sobre el cambio de topología.

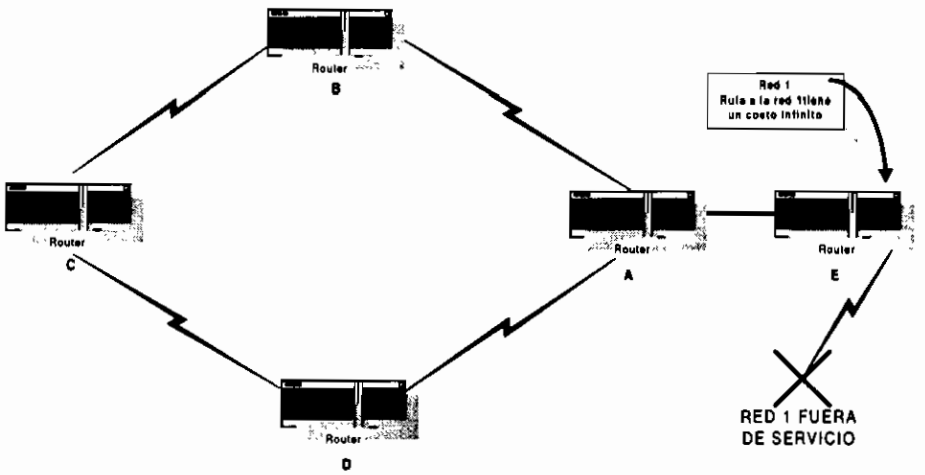


***Figura 1.43** Utilización de envenenamiento de ruta para solucionar el problema de actualizaciones inconsistentes al utilizar la técnica de vector de distancia en el descubrimiento de ruta*

La figura 1.43 provee el siguiente ejemplo. Cuando la red 1 cae, el ruteador E inicia el proceso de envenenamiento de ruta por ingreso de costo infinito en su tabla para la red 1. Debido a que la red 1 se indica como "envenenada", el ruteador E no es susceptible a otras actualizaciones incorrectas acerca de la red 1 que venga de los ruteadores vecinos que podrían clamar tener un camino alternativo válido.

El ruteador E guarda su entrada de ruta envenenada durante algunos ciclos de actualización. Después de una cantidad de tiempo variable, el ruteador envenenado puede disparar una actualización sobre la red 1 en los vecinos del ruteador E (así como a los otros ruteadores en la internet). Todos los ruteadores recalculan sus tablas de vector de distancia y convergen sobre el cambio de topología.

Solución: Temporizadores de *hold-down*

Se puede evitar el problema de cuenta al infinito utilizando temporizadores de *hold-down* los cuales funcionan como sigue:

- Cuando un ruteador recibe una actualización desde su vecino indicando que una red previamente accesible ahora ya no lo es, el ruteador marca la ruta como inaccesible y arranca el temporizador de *hold-down*. Si en cualquier momento antes de que el temporizador expire, una actualización es recibida desde el mismo vecino indicando que la red es otra vez accesible, el ruteador marca la red como accesible y remueve el temporizador de *hold-down*.

• Si una actualización llega desde un ruteador vecino diferente con una métrica mejor que la grabada originalmente para la red, el ruteador marca la red como accesible y remueve el temporizador de *hold-down*.

• Si en cualquier momento antes de que el temporizador expire, una actualización es recibida de un ruteador vecino diferente con una métrica peor, la actualización es ignorada. Ignorar una actualización con una métrica peor cuando el *hold-down* está en efecto permite más tiempo para el reconocimiento de un cambio corrupto a propagarse en toda la internet.

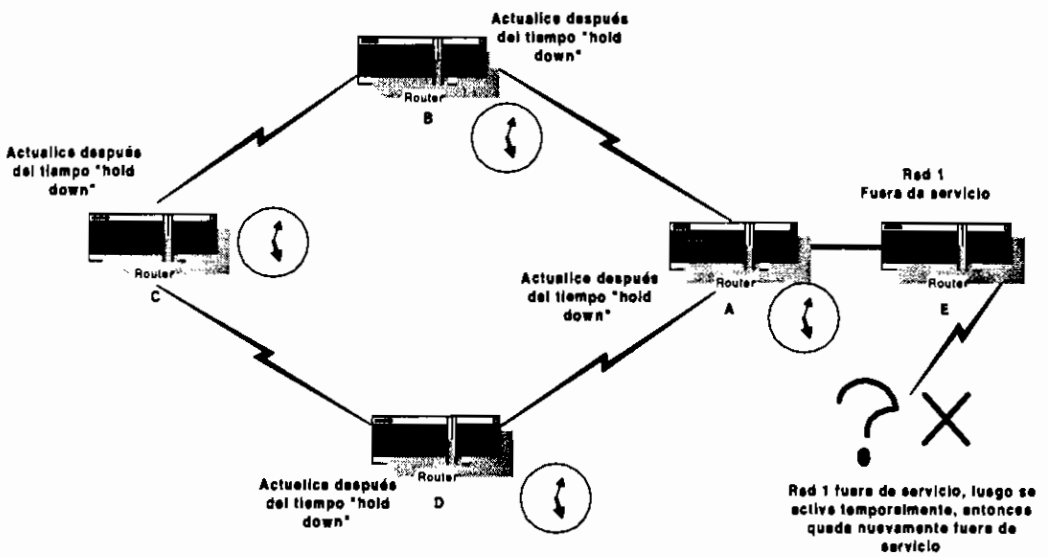


***Figura 1.44** Utilización de temporizadores como solución a problemas de cuenta al infinito al utilizar la técnica de vector de distancia en el descubrimiento de ruta*

b. Estado de enlace

El descubrimiento de ruta basado en estado de enlace - conocido también como *Shortest Path First (SPF)* - mantiene una base de datos compleja de la información de la topología. Puesto que la técnica de vector de distancia tiene información no especificada sobre las redes distantes y no conoce sobre los ruteadores distantes, el descubrimiento de ruta utilizando estado de enlace mantiene completo conocimiento de los ruteadores distantes y de su interconexión.

El descubrimiento de ruta de estado de enlace utiliza paquetes de estado de enlace (LPSs), una base de datos topológica, el algoritmo SPF, el árbol resultante SPF, y finalmente una tabla de enrutamiento de caminos y pórticos a cada red. Más adelante se cubrirán estos temas con más detalle.

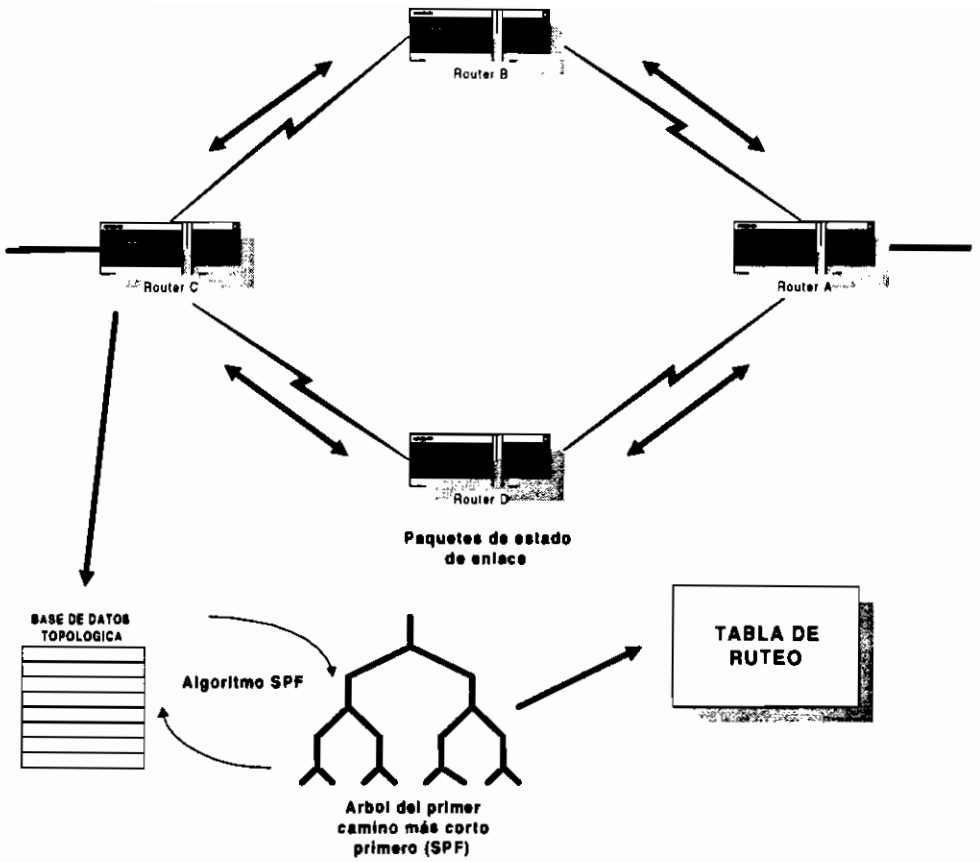


Figura 1.45 Descubrimiento de ruta utilizando la técnica de estado de enlace

b.1 Descubrimiento de red utilizando estado de enlace

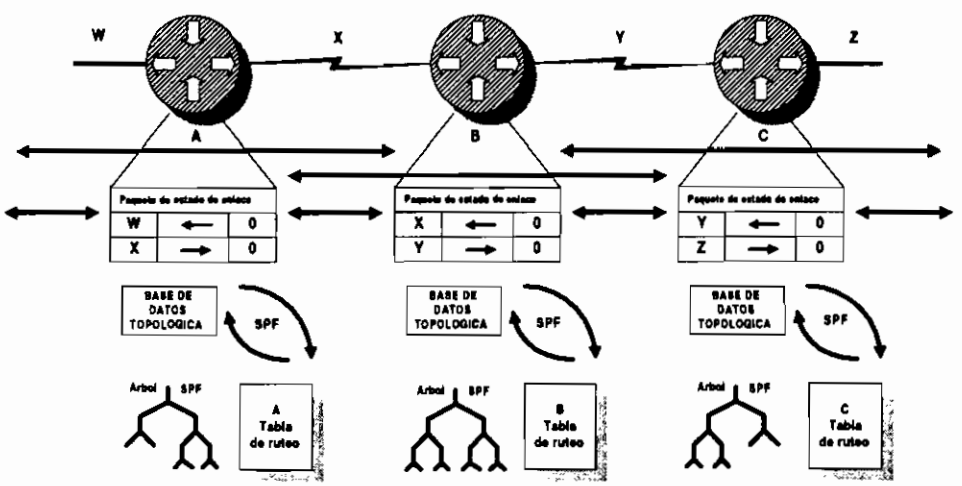


Figura 1.46 Proceso de descubrimiento de ruta utilizando la técnica de estado de enlace

El descubrimiento de ruta con estado de enlace utiliza los siguientes procesos:

- Los ruteadores cambian LSPs (paquetes de estado de enlace) con cada uno de los otros. Cada ruteador comienza con redes directamente conectadas para tener con ellas información de estado de enlace.
- A continuación, cada ruteador en paralelo con cualquier otro, construye una base de datos topológica de todos los LSPs de la internet.
- El algoritmo SPF (o de estado de enlace) calcula la factibilidad de alcanzar una red, determinando el primer camino más corto a cada una de las otras redes en el protocolo de estado de enlace.
- El ruteador construye esta topología lógica de los caminos más cortos como un árbol SPF. Consigo mismo como raíz, el árbol expresa caminos desde el ruteador a todos los destinos.
- Finalmente, el ruteador lista sus mejores caminos y pórticos a esas redes destino en la tabla de ruteo. El ruteador también mantiene otras bases de datos de elementos de la topología y sus estados en detalle.

Después que los ruteadores descubren dinámicamente los detalles de sus internets, ellos pueden usar la tabla de ruteo para la conmutación de tráfico de paquetes.

b.2 Actualización ante cambios de topología usando estado de enlace

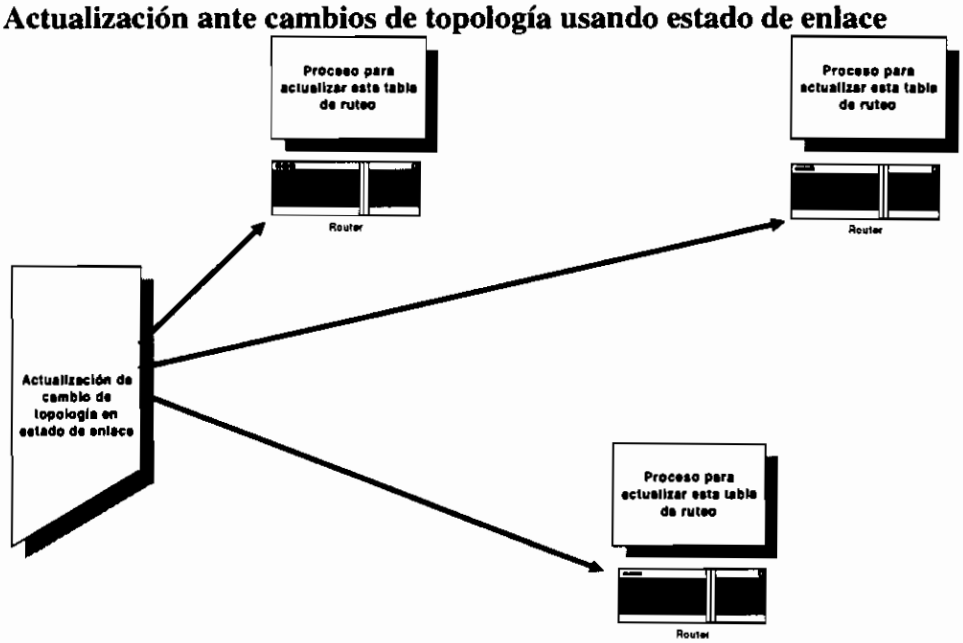


Figura 1.47 Actualización de tablas de ruta al utilizar la técnica de estado de enlace en el descubrimiento de ruta cuando ocurre un cambio de topología

Los algoritmos de estado de enlace confían en la utilización de la misma actualización de estado de enlace. Cuando una topología de estado de enlace cambia, los ruteadores que primero se dan cuenta del cambio

envían información a otros ruteadores o a un ruteador designado al que todos los ruteadores utilizan para su actualización. Esto determina la propagación de información de ruteo común a todos los ruteadores en la internet. Para conseguir la convergencia, cada ruteador hace lo siguiente:

- Guarda la pista de sus vecinos: el nombre del ruteador vecino, cuando el vecino está en o fuera de servicio, y el costo del enlace a su vecino.
- Construye un LSP que lista los nombres de sus vecinos y sus costos de enlace. Esto incluye nuevos vecinos, cambios en los costos de enlace, y enlaces a vecinos que están fuera de servicio.
- El ruteador envía este LSP a todos los ruteadores que lo reciban.
- Cuando un ruteador recibe el LSP, lo graba en su base de datos manteniendo de esta manera el más reciente LSP generado desde otro ruteador.
- Utilizando los datos de los LSP acumulados, se construye un mapa completo de la topología de internet, procediendo desde un punto de arranque común para luego utilizar el algoritmo SPF y calcular las rutas a cada red de destino.

Cada vez que un LSP provoca un cambio en la base de datos de estado de enlace, el algoritmo de estado de enlace (o SPF) recalcula el mejor camino y actualiza la tabla de ruteo. Entonces cada ruteador toma en cuenta el cambio de topología para determinar el camino más corto a utilizar en la conmutación de paquetes.

Requerimientos de estado de enlace

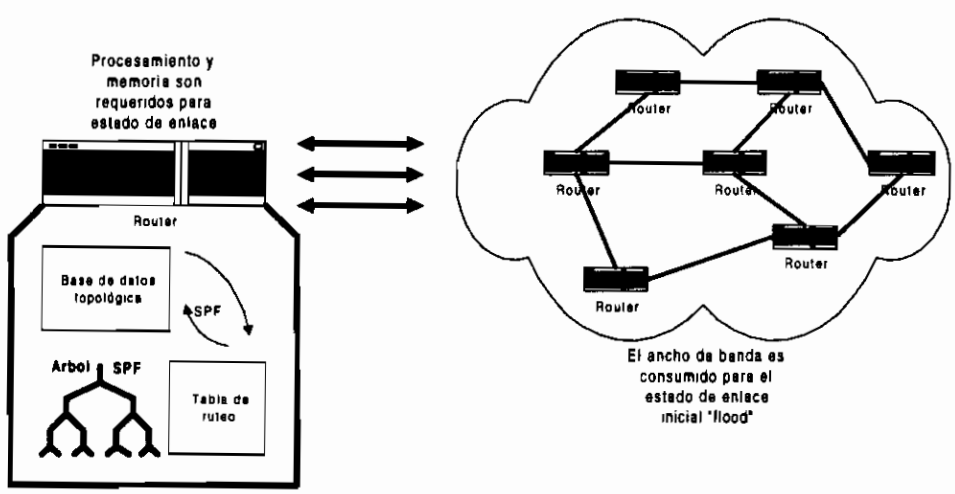


Figura 1.48 Recursos que ocupa la técnica de estado de enlace en el descubrimiento de rutas

Se hará referencia a dos tipos de requerimientos que son determinantes cuando se utiliza estado de enlace:

1. Requerimientos de memoria y procesamiento
2. Requerimientos de ancho de banda

Cuando se utilizan protocolos de enrutamiento de estado de enlace, se debe garantizar que los ruteadores que se elijan sean capaces de proveer recursos suficientes para funciones que utilizan memoria y procesamiento.

Los ruteadores mantienen información de sus vecinos y de las redes que pueden alcanzar a través de otros nodos de ruteo. Para enrutamiento de estado de enlace, la memoria debe retener información de varias bases de datos, del árbol de topología y de la tabla de ruteo.

Una causa para referirnos a la utilización del ancho de banda requerido por el enrutamiento de estado de enlace, es la inundación *(flooding)* de paquetes de estado de enlace inicial. Durante el proceso de descubrimiento inicial, todos los ruteadores usan protocolos de enrutamiento de estado de enlace enviando LSPs a los otros ruteadores. Esta acción inunda la internet provocando demandas pico de ancho de banda, y reduciendo temporalmente el ancho de banda disponible para el tráfico ruteado que lleva datos de usuario.

Luego de esta inundación inicial, los protocolos de enrutamiento de estado de enlace generalmente requieren de ancho de banda para enviar sus LPS cuando ocurre un cambio en la topología.

Problemas: Actualizaciones de estado de enlace

El aspecto más complejo y crítico del enrutamiento que utiliza estado de enlace es asegurar que todos los ruteadores hayan obtenido los LPSs necesarios. Los ruteadores con diferentes configuraciones de LPSs calcularán rutas basadas sobre datos de topología diferentes. Entonces las rutas comienzan a ser inalcanzables como un resultado de la degradación de las rutas de enlace. Por ejemplo:

- Supongamos que la red 1 entre los ruteadores C y D (ver Figura 1.49) esté fuera de servicio. Como se mencionó anteriormente, los dos ruteadores construyen un LSP para reflejar el estado inalcanzable de la red 1.
- Pronto la red 1 se recupera y es necesario que otro LSP refleje el nuevo cambio en la topología.
- Si el mensaje inicial de "la red 1 inalcanzable" desde el ruteador C utiliza un camino lento para su actualización, el último mensaje "red 1 alcanzable" proveniente del ruteador D podría llegar antes que el mensaje inicial de C.

- Con los LSPs no sincronizados, el ruteador A puede encarar un dilema acerca de cual árbol SPF utilizar para construir su tabla, utilizando el dato que proviene de D o el que proviene de C.

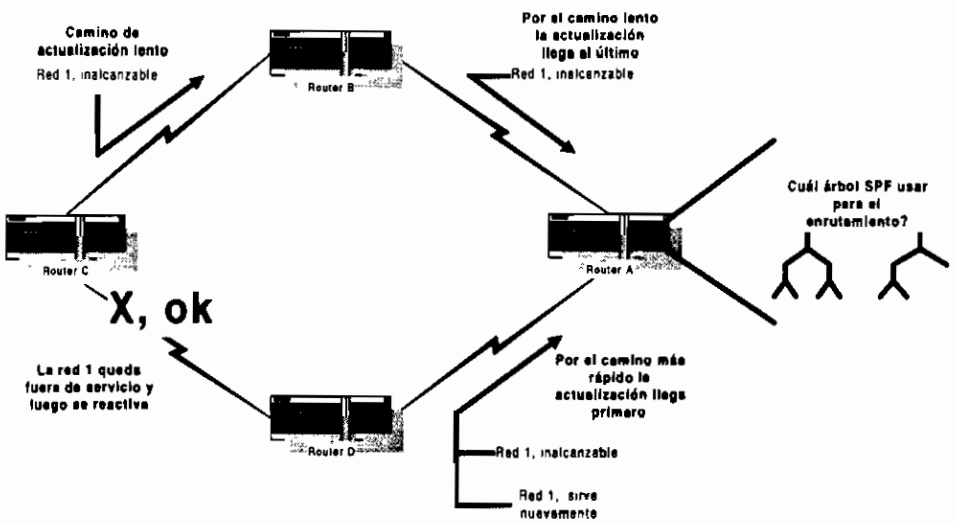


***Figura 1.49** Problema de actualización lenta de rutas al utilizar técnica de estado de enlace en el descubrimiento de ruta*

Si la distribución de LSPs (paquetes de estado de enlace) a todos los ruteadores no es realizada correctamente, el enrutamiento de estado de enlace puede resultar en rutas inválidas.

Implementar protocolos de estado de enlace sobre redes de tamaño muy grande puede intensificar el problema de fallas en la distribución de paquetes de estado de enlace.

Si una parte de la internet se pone en funcionamiento primero con otras partes por funcionar más tarde, el orden de envíos y recepciones de LSPs variará. Esta variación puede alterar e impedir la convergencia. Los ruteadores podrían aprender acerca de diferentes versiones de la topología antes de construir sus árboles SPF y tablas de ruta.

Sobre una gran internet, las partes que se actualizan más rápidamente pueden causar problemas a las partes que se actualizan más lentamente. Cuando se producen actualizaciones fallidas, los LSPs pueden multiplicarse propagándose a lo largo de la red, consumiendo improductivamente cada vez más ancho de banda.

Eventualmente una partición puede dividir la internet en dos partes: una que se actualiza rápidamente y otra que lo hace lentamente. Se deberá entonces devolver a la red una interconectividad aceptable superando las complejidades de los enrutamientos de estado de enlace.

Solución: Mecanismos de estado de enlace

Los mecanismos para la solución de los problemas que se producen en el enrutamiento de estado de enlace buscan lo siguiente:

1. Reducir la necesidad de recursos
2. Coordinar las actualizaciones de estado de enlace

Para conseguir esto, los procesos en más detalle se describen a continuación:

- Los administradores de red pueden reducir la distribución periódica de LSPs, haciendo que las actualizaciones ocurran en períodos más largos, utilizando una duración configurable. El *dampening* no interfiere con las actualizaciones LSP disparadas por cambios de topología.
- Las actualizaciones LSP pueden ir a un "grupo de multilanzamiento (*multicast*)" antes que "inunden (*flooding*)" a todos los ruteadores. Sobre las LANs interconectadas, se puede usar uno o más ruteadores diseñados como depositarios destino para las transmisiones LSP. Otros ruteadores pueden usar sus ruteadores designados como una fuente especializada de datos de topología consistente.
- En grandes redes se puede configurar una jerarquía que consista de varios niveles de ruteadores. Un ruteador en una área de los dominios de la jerarquía no necesita almacenar y procesar LSPs desde otros ruteadores no localizados en su área.
- Para problemas de coordinación LSP, las implementaciones de estado de enlace pueden permitir marcas (*stamps*) de tiempo LSP, números de secuencia, y otros mecanismos relativos para evitar distribución de LSP inexacta o actualizaciones descoordinadas.
- El particionamiento de una internet puede ser activamente manejada con una jerarquía si el protocolo de estado de enlace provee de administración jerárquica. Entonces los ruteadores podrán concentrarse únicamente en su dominio jerárquico o área, y pueden depender de ruteadores especiales ubicados en los bordes de dominio para información de ruteo externo.

Comparación entre enrutamiento de estado de enlace y vector de distancia

- El enrutamiento de vector de distancia obtiene todos los datos de topología (tablas de ruteo) que sus ruteadores vecinos procesaron. El enrutamiento de estado de enlace obtiene un vista amplia de la topología de red entera por acumulación de todos los LSPs necesarios.
- El descubrimiento por vector de distancia determina el mejor camino añadiendo a la métrica valores que recibe como tablas movidas de ruteador a ruteador. Para el descubrimiento por estado de enlace, cada ruteador trabaja en paralelo para calcular su propio camino más corto a los destinos.

- Con vector de distancia, las actualizaciones de tablas se hacen de ruteador a ruteador siendo frecuentes y periódicas, lo que determina un proceso de convergencia lenta. Para estado de enlace las actualizaciones se realizan únicamente cuando se detecta cambios en la topología, pasando LSPs relativamente pequeños a todos los otros ruteadores, o a un grupo de multilanzamiento, determinando por lo general que el proceso de convergencia sea más rápido.

Vector de distancia	Estado de enlace
Vistas de la topología de red desde la perspectiva de los vecinos	Obtiene una vista común de la topología de la red entera
Añade vectores de distancia de ruteador a ruteador	Calcula el camino más corto a los otros ruteadores
Actualizaciones periódicas y frecuentes: convergencia lenta	Actualizaciones eventuales: convergencia rápida
Pasa copias de las tablas de ruteo a los ruteadores vecinos (más próximos)	Pasa actualizaciones de enrutamiento de estado de enlace a otros ruteadores

***Tabla 1.19** Comparación entre vector de distancia y estado de enlace como técnicas de descubrimiento de ruta*

c. Híbrido balanceado

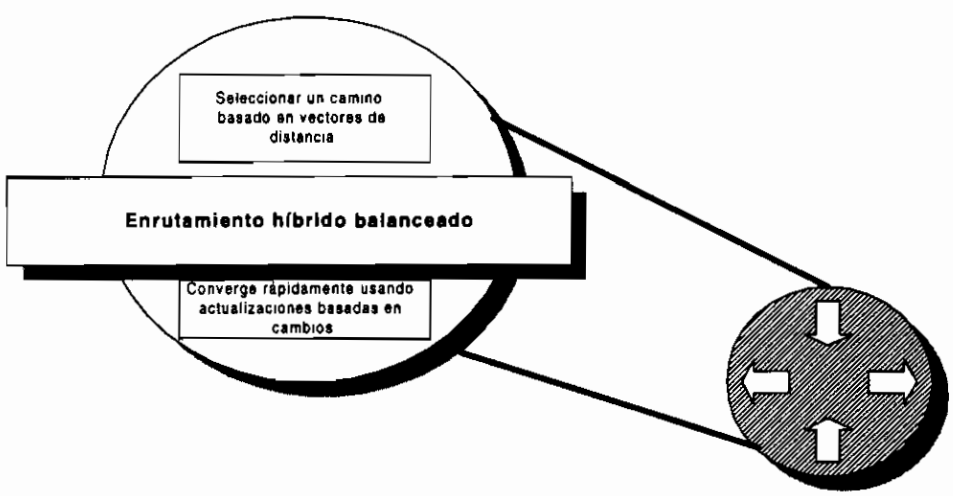


***Figura 1.50** Enrutamiento híbrido balanceado*

Esta tercera técnica que utilizan los protocolos de enrutamiento combina aspectos tanto de vector de distancia como de estado de enlace.

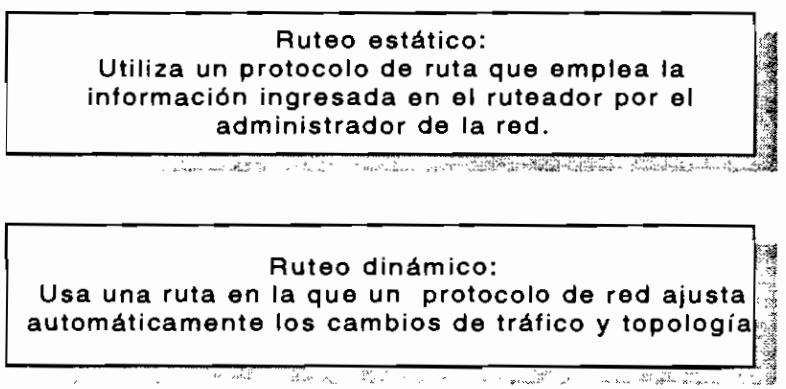
La técnica de enrutamiento *híbrido balanceada* utiliza vectores de distancia para determinar los mejores caminos a las redes destino. Sin embargo, difiere de la técnica de vector de distancia en que utiliza los

cambios de topología para disparar actualizaciones de la base de datos de enrutamiento (como en la técnica de estado de enlace).

El enrutamiento híbrido balanceado converge rápidamente, como los protocolos de estado de enlace. Sin embargo, se diferencia de estos últimos en que se hace énfasis en el ahorro de recursos tales como ancho de banda, memoria y sobrecarga del procesador.

B.4 Selección de ruta

Una vez que por medio de técnicas de descubrimiento de ruta se logran determinar tablas de ruteo, se puede utilizar la información de costos para calcular el mejor recorrido a través de la internet.



La selección de las rutas puede ser dinámica, de forma que el ruteador pueda adaptarse constantemente a las condiciones cambiantes de la red o estática, haciendo que los paquetes de datos sigan siempre un camino determinado.

Tipos de selección de ruta

a. Selección de ruta estática

La técnica de selección de rutas estática es administrada manualmente; un administrador de red realiza configuraciones al ruteador. El administrador debe actualizar manualmente la ruta estática cuando la topología de la red cambia y requiere de actualización. No se permite tomar decisiones a los ruteadores intermedios. El ruteo estático es privado y no conviene tener ruteadores externos como parte del proceso de actualización manual.

Nota: La técnica de selección de ruta estática no utiliza protocolos de descubrimiento de ruta (vector de distancia, estado de enlace ó híbrido) como apoyo, porque no los necesita.

Aplicaciones:

a)

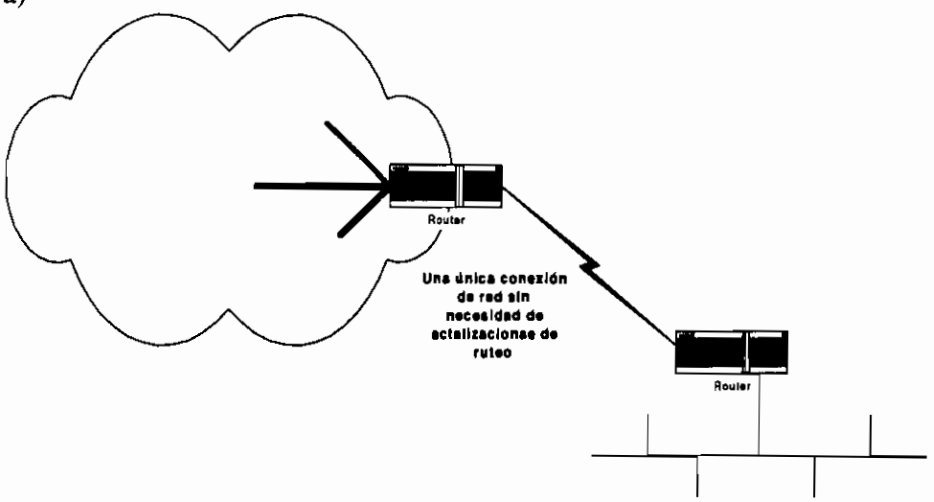


Figura 1.51 Aplicación de rutas estáticas en enlaces punto a punto

Cuando el administrador tiene un conocimiento claro sobre la topología (mapa) de la red, el ruteo o selección de ruta estática puede ser de gran utilidad.

El ruteo dinámico tiende a revelar la estructura de la internet. Por razones de seguridad, es apropiado ocultar partes de la internet. El ruteo estático permite que el administrador de la red determine que partes de la red sean accesibles y otras sean restringidas.

b)

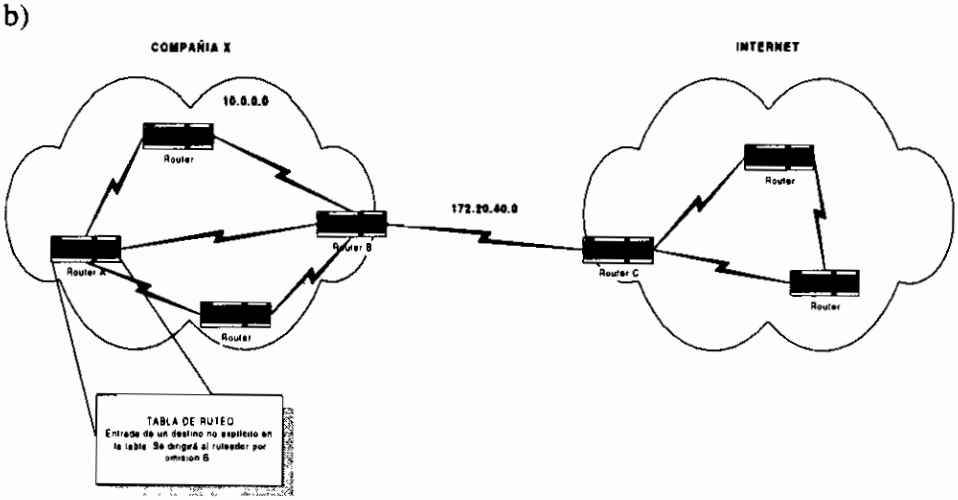


Figura 1.52 Aplicación de la definición de ruta por default

La figura 1.52 muestra una aplicación para una ruta por *default*, la cual es una entrada en la tabla de enrutamiento que es usada para direccionar tramas, para las cuales el próximo salto no es explícitamente listado en la tabla. Las rutas por *default* pueden ser designadas por una configuración

estática realizada por el administrador, o designadas por ruteo dinámico con conocimiento de muchos protocolos.

En el ejemplo de la figura 1.52, los ruteadores de la compañía X poseen conocimiento específico de la topología de la red de la compañía X, pero no de otras redes. El mantener conocimiento de cada una de las otras redes de la internet se volvería innecesario e irracional, sino imposible.

Por el contrario, el mantener un conocimiento de la red interna, en donde cada ruteador de la compañía X es informado de la ruta por *default* que puede alcanzar en el caso de un destino desconocido, para que éste se encargue de direccionar el paquete a la internet, resulta muy conveniente.

c)

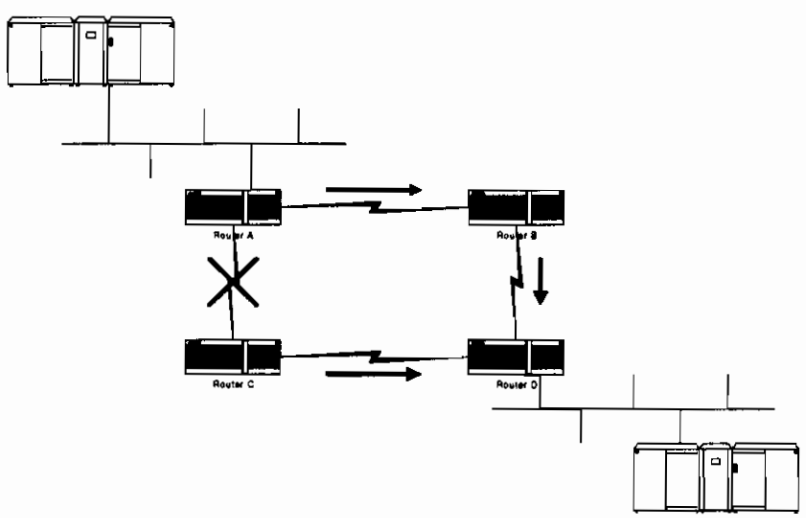


***Figura 1.53** Desventaja del enrutamiento estático*

Si bien se han descrito algunas aplicaciones en las que resultaría útil la selección de ruta estática, también puede darse el caso en el que esa técnica resulte inconveniente. Supongamos el caso de la figura 1.53, donde el ruteador A tiene configurada su ruta por *default* en el puerto conectado a C, y supongamos que el enlace entre A y C se pierde, todos los paquetes que bien podrían ser direccionador por el puerto que enlaza A con B para llegar al destino D tendrían que esperar hasta que el enlace A-C se active o hasta que el ruteador sea configurado manualmente. Esto no sucedería con la selección de ruta dinámica ya que ofrece flexibilidad automática.

b. Selección de ruta dinámica

La selección de ruta dinámica permite que luego de que el administrador de la red ingrese comandos de configuración, el ruteador arranque con el ruteo dinámico. La ruta es actualizada automáticamente por un proceso

de enrutamiento donde la información de nueva topología es recibida de la propia red. Los cambios en el enrutamiento dinámico son realizados entre ruteadores como parte de un proceso de actualización.

La selección de ruta dinámica utiliza algoritmos de asignación de ruta que recogen información de los costos continuamente. Se asigna una ruta a cada paquete en función de los últimos costos de descubrimiento de ruta. Se pueden utilizar diferentes rutas para enviar paquetes entre dos dispositivos, dependiendo del estado cambiante de la red. Además, cada ruteador se encarga de seleccionar la ruta que tomará cada paquete, seleccionando de esta forma la próxima parada que tendrá cada uno de los paquetes antes de que se elija la nueva ruta que deberá tomar.

b.1 Operaciones de descubrimiento de ruta que requiere la selección de ruta dinámica

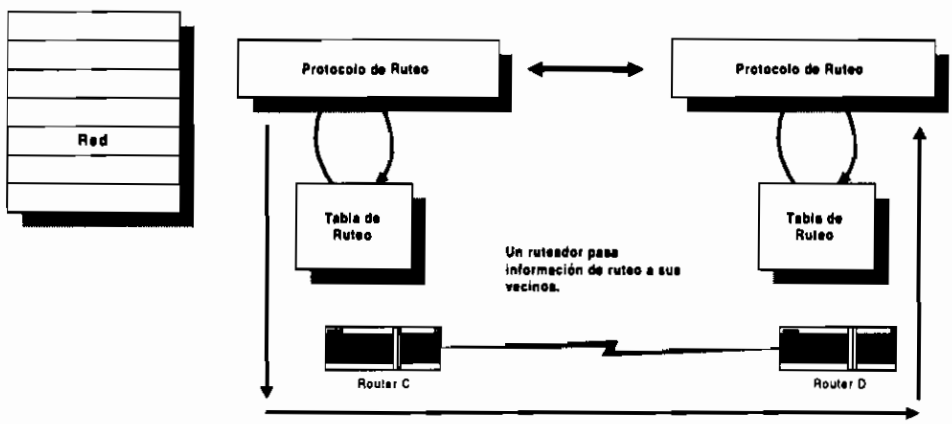


Figura 1.54 Operaciones del descubrimiento de ruta en enrutamiento dinámico

El éxito de la selección de ruta dinámica depende de dos funciones básicas del ruteador:

- Mantener una tabla de enrutamiento
- Actualizar las tablas de enrutamiento a otros ruteadores

Al contrario de la selección de ruta estática que nunca envía actualizaciones, la selección de ruta dinámica utiliza protocolos basados en descubrimiento de ruta (sean de vector de distancia, estado de enlace o híbridos) para repartir el conocimiento de rutas expresadas en tablas de enrutamiento. El protocolo de descubrimiento de rutas define el grupo de reglas usadas por un ruteador cuando se comunica con sus ruteadores vecinos.

b.2 Utilizando métricas para representar distancia

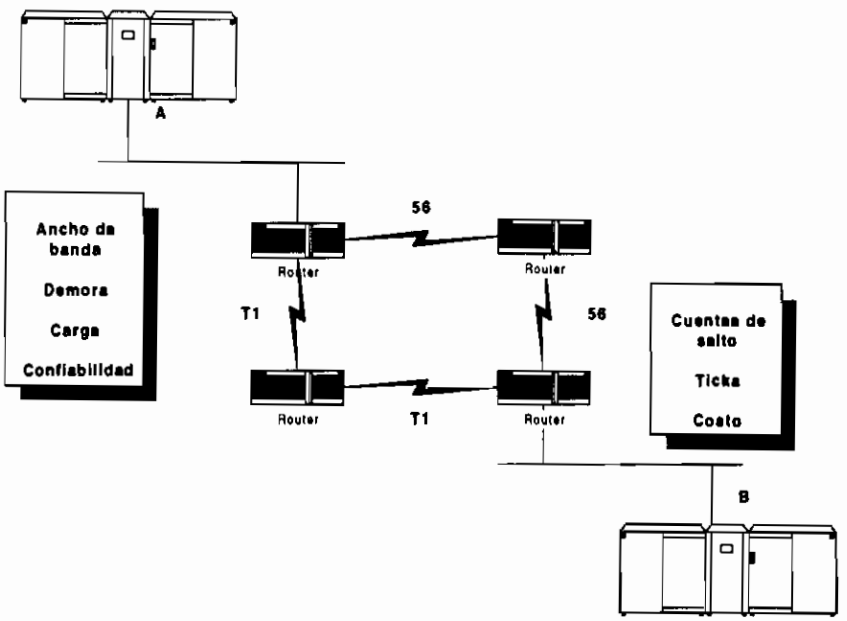


Figura 1.55 Determinación de métricas

Cuando un algoritmo de descubrimiento de ruta (o enrutamiento) actualiza la tabla de enrutamiento (o ruteo), su objetivo primario es determinar la mejor información a ser incluida en la tabla. El algoritmo genera un número llamado valor de la métrica para cada ruta a través de la red. Típicamente, la métrica más pequeña es el mejor camino.

Las métricas pueden ser calculadas basándose en una única característica del camino. Se pueden hacer cálculos más complejos utilizando varias características. A continuación, algunas de las métricas más comúnmente utilizadas por los ruteadores:

- Ancho de banda- Capacidad de datos de un enlace. Por ejemplo, un enlace *Ethernet* de 10 Mbps es preferible a un enlace dedicado de 64 Kbps.
- Demora- Longitud de tiempo requerida para mover un paquete desde su origen a su destino.
- Carga- Cantidad de actividad sobre los recursos de la red tales como un ruteador o un enlace.
- Confiabilidad- Usualmente se refiere a la tasa de errores de bits (Bits Error Rate) de cada enlace de red.
- Cuenta de saltos- El número de pasos de un paquete a partir del puerto de salida de un ruteador.
- Ticks- Espera sobre un enlace de datos utilizando un reloj de *ticks* (1 *tick* aproximadamente 55 ms) de un PC IBM.

- Costo- Valor arbitrario, usualmente basado en el ancho de banda, valor del dólar, u otra medida, que es asignada por el administrador de la red.

B.5 Servicios de conexión

Como ya se hizo referencia en el subnivel enlace de datos LLC, los servicios de conexión a ese nivel se encargaban de controlar la cantidad de datos transmitidos entre dos dispositivos y la notificación de las tramas perdidas o mezcladas. Los servicios de conexión del nivel red se basan en estas funciones y se suelen utilizar cuando no se emplean los servicios del subnivel enlace de datos LLC para brindar mayor fiabilidad.

Recuérdese que existen tres tipos de servicios de conexión:

1. Servicios sin conexión y sin reconocimiento
2. Servicios sin conexión y con reconocimiento
3. Servicios orientados a conexión

Las técnicas de servicios de conexión fueron tratadas en detalle en el tema del nivel enlace de datos, en el subnivel LLC.

Técnicas de control de servicios en el nivel red

Los servicios de conexión al nivel red también utilizan los reconocimientos que proporciona el subnivel enlace de datos LLC. Los reconocimientos proporcionan las siguientes técnicas de servicios de conexión del nivel red:

a. Control de flujo a nivel de red

Controlan la cantidad de datos que siguen una ruta específica de la red (se denomina también control de congestión). La diferencia principal con el control de flujo al nivel enlace de datos (que utiliza el control de flujo en función de las capacidades del dispositivo), es que el control de flujo al nivel red se basa en las capacidades de la internet.

Por lo general, una internet utiliza un número elevado de dispositivos. Por tanto, dependiendo del tráfico que generen emisores y receptores, las velocidades de transmisión y la fiabilidad de la red son cambiantes. El control de flujo al nivel red incluye los mecanismos que se usan para controlar la cantidad de datos que se envían en una ruta determinada.

El control de flujo al nivel red puede implicar una selección inteligente del recorrido. Debido a que trata la congestión de la red, el control de flujo al nivel red es conocido como control de congestión.

El control de flujo al nivel red se puede realizar con negociación de velocidad garantizada mediante ventanas estáticas y dinámicas. En

ocasiones, los reconocimientos que utiliza el control de flujo de ventana se demoran, provocando que el emisor no pueda diferenciar si un error de la red ha provocado que se pierda el reconocimiento o si la congestión de la red lo ha demorado tanto que sobrepasa el tiempo límite del emisor. Por esta razón, algunos protocolos implementan paquetes especiales para indicar la congestión de la red entre dispositivos intermedios.

b. Control de errores al nivel red

Está relacionado principalmente con:

- Pérdida de paquetes
- Duplicación de paquetes
- Datos alterados

Si bien las dos primeras condiciones de error se pueden enfrentar con la utilización de los números de secuencia y los reconocimientos, esta tarea la suele realizar el nivel transporte. El tercer problema suele abordarse mediante la utilización de CRC (*Cyclic Redundancy Check*) u otra suma de comprobación al paquete. Estas sumas se calculan únicamente en cada salto (calculan solamente las sumas de comprobación de los datos) debido a que los campos de dirección del encabezamiento del paquete cambia en cada punto de asignación de ruta.

c. Control de secuencia de paquetes en el nivel red

El control de secuencia fue tratado en el tema relacionado a "Técnicas de servicios de conexión" en el nivel enlace de datos. Como se mencionó, el nivel enlace de datos no realiza control de secuencia de paquetes, y a pesar de que este tipo de control puede ser implementado en el nivel red, esta tarea es generalmente implementada en el nivel transporte.

B.6 Servicios de *Gateway* en el nivel red

Los servicios de *gateway* son implementados para interpretar y traducir las normas de dos redes distintas, es decir dos redes que utilizan diferentes normas de direccionamiento, descubrimiento de ruta, selección de ruta y servicios de conexión.

Supongamos dos redes que segmentan unidades de datos con tamaños diferentes. Los servicios de *gateway* en el nivel red se encargarán de la fragmentación y reconstrucción de los datos en tamaños aceptables para ambas redes. Conforme el *gateway* ajusta los tamaños de paquetes de datos, debe también garantizar los requisitos de servicios de conexión de cada red, como el control de errores y secuenciamiento de paquetes.

Se debe observar que la implementación de los servicios de *gateway* se puede realizar en cualquier nivel del modelo OSI, ya que un *gateway* es un dispositivo o aplicación que

traduce una serie de normas a otras. Sin embargo la mayor parte de implementaciones se realizan en los niveles superiores del modelo OSI.

1.2.5.4 Niveles superiores y aplicaciones del modelo de referencia OSI

Se ha visto como los niveles físico y de enlace de datos se encargan de garantizar básicamente la transmisión de datos, el nivel red garantiza fundamentalmente el ruteo y enrutamiento.

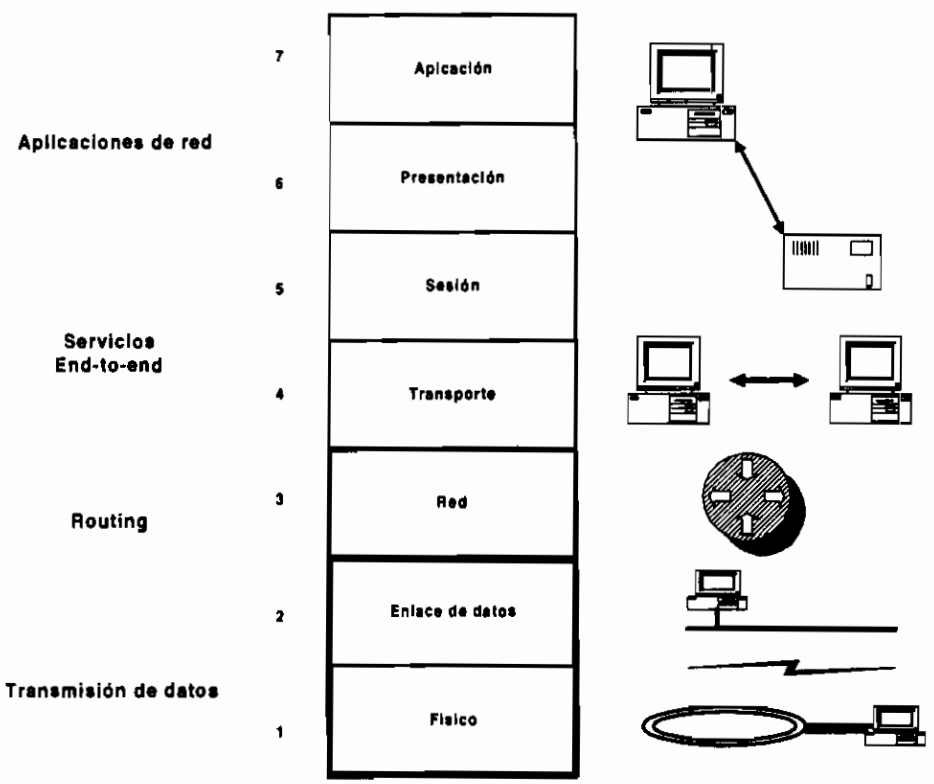


Figura 1.56 Modelo de referencia OSI y sus capas superiores o de aplicación

A continuación se verá la forma en que las capas superiores (4,5,6 y 7) se encargan de garantizar los servicios de extremo a extremo (dispositivos no incluidos ni en el subsistema de conectividad ni en el de infraestructura de transporte), y las aplicaciones de red.

Debido a que el presente estudio está orientado a las funciones realizadas por las tres primeras capas del modelo OSI, los siguientes niveles serán considerados de manera resumida.

A. El nivel transporte OSI

El nivel transporte se encargará fundamentalmente de garantizar:

1. Segmentación de datos de las capas superiores
2. Establecer la conexión extremo a extremo
3. Enviar segmentos de un *host* extremo a otro
4. Opcionalmente, asegurar la integridad de datos

Los servicios de transporte permiten a los usuarios segmentar y reensamblar algunas aplicaciones sobre el mismo grupo de datos de la capa transporte.

Este grupo de datos de la capa transporte provee servicios de transporte extremo-a-extremo (*end-to-end*); esto constituye una conexión lógica entre los puntos extremos de la internet: el dispositivo fuente y el dispositivo destino.

Como la capa transporte envía sus segmentos, aquella puede también asegurar la integridad de datos. Un método lo provee el control de flujo. El control de flujo evita el problema de que un dispositivo en un lado de la conexión determine un sobreflujo en los *buffers* del dispositivo del otro lado de la conexión. El sobreflujo puede causar pérdida de datos.

Los servicios de transporte permiten también a los usuarios requerir transporte de datos confiable entre sistemas extremos que se comunican. El transporte confiable utiliza un servicio orientado a conexión entre los sistemas extremos que se comunican, para cumplir lo siguiente:

- Asegurar que los segmentos entregados devuelvan un reconocimiento al emisor
- Proveer la retransmisión de cualquier segmento que no sea reconocido
- Poner los segmentos en el orden de secuencia correcto en el destino

En sí, el nivel transporte está diseñado para ocultar al proceso de nivel superior la complejidad de la estructura de red de computadores. Se encarga de compensar la falta de servicios de conexión fiables u orientados a la conexión de los niveles inferiores. El término fiable no garantiza que se entreguen los datos, pues si se rompiera el cable, el nivel transporte no puede garantizar la entrega de datos. Aún así, las implementaciones fiables del nivel transporte pueden confirmar o denegar la entrega de datos.

A.1 Multiplexación de aplicaciones

Una de las principales razones para la división en capas del modelo de referencia OSI es permitir que múltiples aplicaciones utilicen el mismo protocolo de transporte.

Una vez que se ejecuta el proceso de multiplexación sobre varias aplicaciones, la única forma de distinguir una aplicación de otra es mediante la identificación de cada unidad de datos con un mecanismo de transición como por ejemplo un número de puerto.

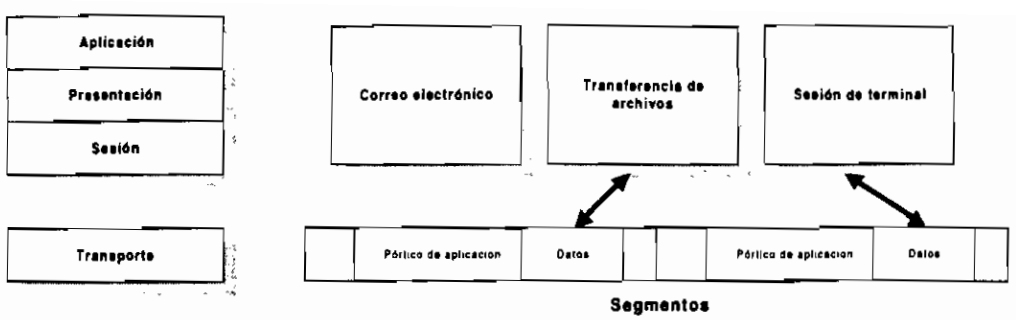


Figura 1.57 Multiplexación de aplicaciones mediante la utilización de números de puerto

El *software* en el ente emisor configura un número de puerto necesario para cada una de las aplicaciones antes de la transmisión. Posteriormente, cada aplicación de *software* que envíe un segmento de un grupo de datos utiliza el mismo puerto previamente definido.

Cuando el ente destino recibe el grupo de datos, éste puede separar y juntar cada uno de los segmentos de las aplicaciones. Esta demultiplexación en el destino permite que la capa transporte pueda pasar los datos a su aplicación par destino.

A.2 Establecimiento de conexión

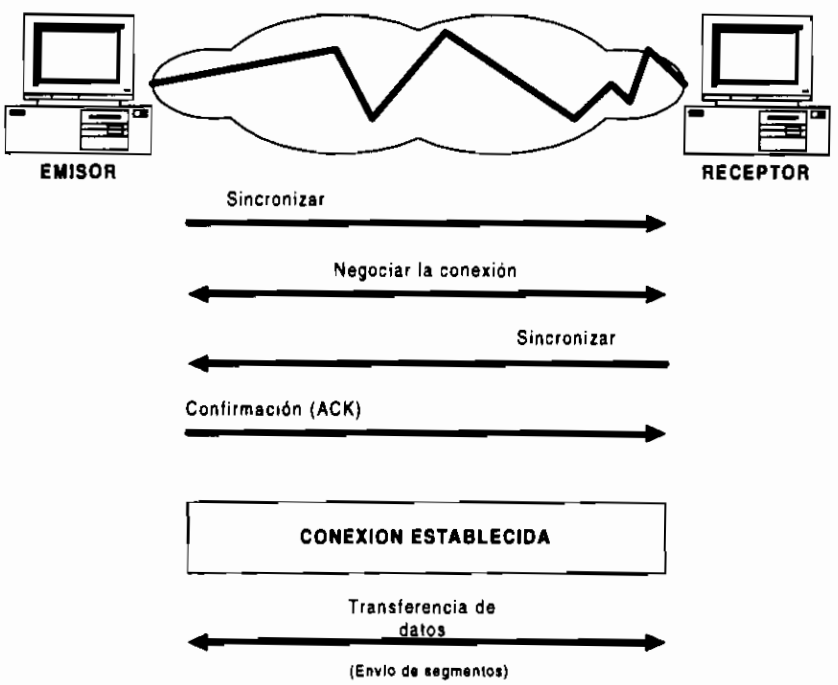


Figura 1.58 Proceso en el establecimiento de una conexión

Para usar servicios de transporte confiables, se debe establecer una sesión orientada a conexión con su sistema par.

Para comenzar la transferencia de datos, los entes emisor y receptor acuerdan iniciar la sesión. El protocolo utiliza mensajes de envío a través de la red para verificar que la transferencia sea autorizada y que ambos lados estén listos.

Luego de que la sincronización ha ocurrido, se dice que la conexión se ha establecido, y que la transferencia de información puede comenzar. Durante la transferencia el protocolo verifica que los datos son recibidos correctamente.

A.2.1 Envío de segmentos con control de flujo

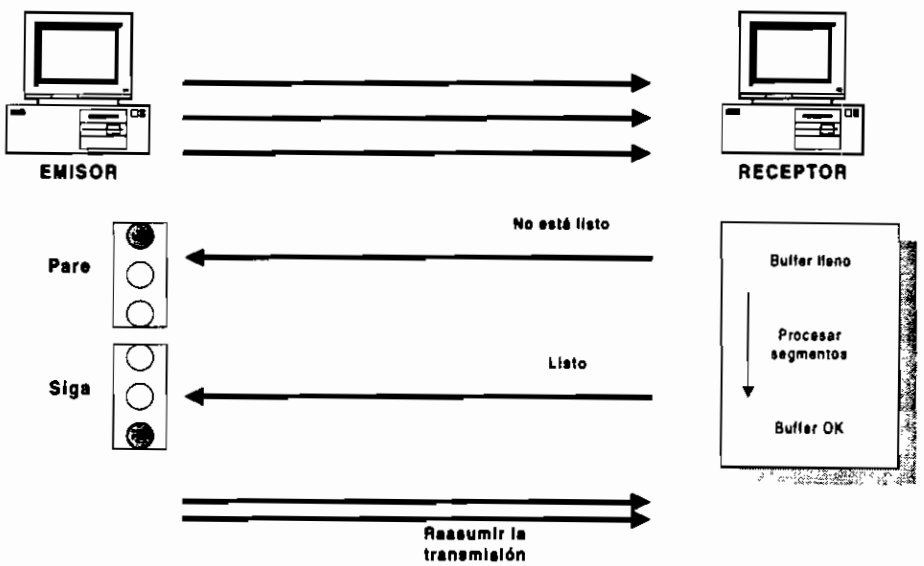


Figura 1.59 Envío de segmento mediante la utilización de control de flujo

La congestión en una red puede aumentar por dos razones:

1. Existe un dispositivo generador de datos que es demasiado rápido para la infraestructura de la red
2. Muchos dispositivos fuente quieren llegar a un mismo dispositivo destino, directamente o a través de un mismo dispositivo intermedio.

Cuando esto sucede, el protocolo correspondiente al nivel transporte tratará de manejar esta situación mediante el control de flujo. Si un ente receptor o intermedio recibe datagramas a ser procesados, aquellos serán almacenados temporalmente en memoria. Si el tamaño de la información que llega es menor que los *buffers* disponibles, el problema es fácilmente solucionado. Si por el contrario, el tamaño de los datos que llegan supera la capacidad de almacenamiento temporal, el dispositivo receptor esperará hasta llenar sus *buffers* y luego enviará una señal de no está listo al emisor para que detenga la transmisión. Una vez que se han procesado los datos almacenados en los *buffers*, el receptor envía otra señal de listo para indicar que está en capacidad de recibir datos.

A.2.2 Utilización de ventanas

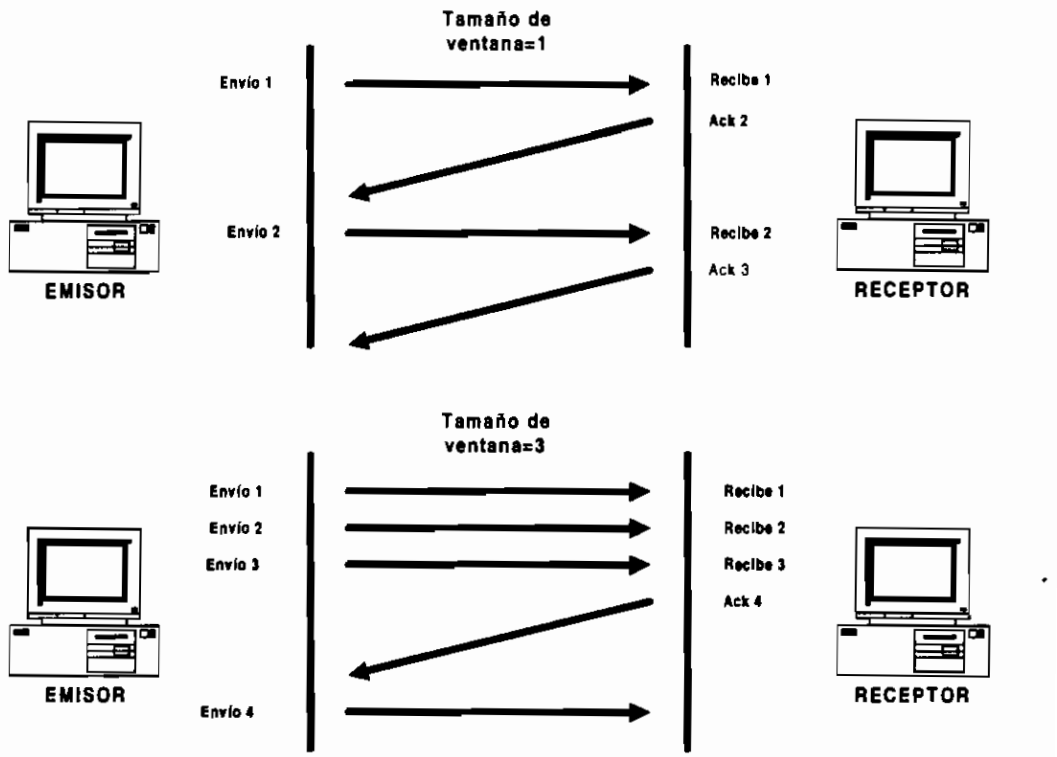


Figura 1.60 Control del proceso de transmisión mediante la utilización de reconocimientos

Es lógico que los segmentos de datos transmitidos tengan que llegar a su destino en el orden correcto, completos y sin duplicación. Una forma sencilla de controlar este proceso de transmisión es mediante la utilización de reconocimientos que envía el receptor al emisor una vez que recibió el paquete correctamente.

Sin embargo, el envío de segmentos puede realizarse más eficientemente si se aprovecha el tiempo en que el emisor envía un segmento y termina de procesar y recibir un reconocimiento. Al número de segmentos que pueden transmitirse mientras el emisor no recibe un reconocimiento, se lo conoce como tamaño de ventana.

En la figura 1.60 se puede observar como en el primer caso se utiliza un ventana de tamaño 1, es decir por cada envío que se realice se espera un reconocimiento. En el segundo caso, el tamaño de ventana es 3, es decir que se realiza el envío de 3 segmentos de datos y se espera un reconocimiento.

A.2.3 Confiabilidad utilizando ventanas

La entrega confiable garantiza que un grupo de datos transmitidos a través de un enlace de datos llegue sin duplicación o pérdida de datos.

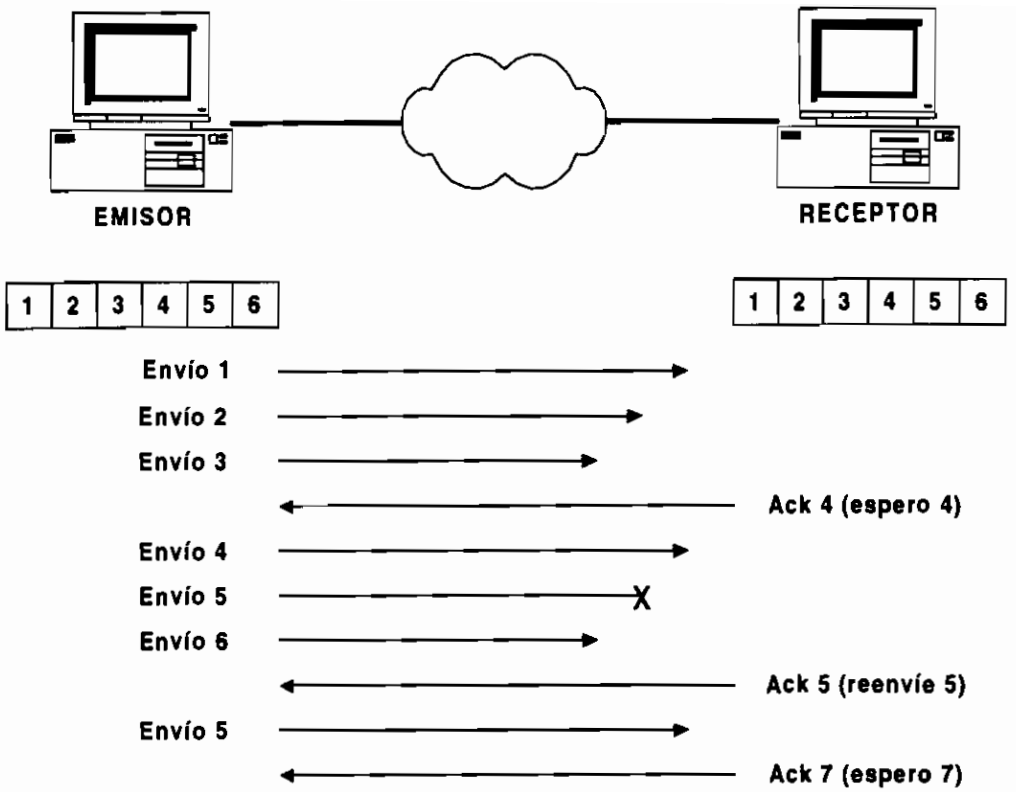


Figura 1.61 Confirmación de la recepción de datos y retransmisión

Para la entrega confiable de grupos de datos se utilizan algunas técnicas. Un ejemplo es el reconocimiento positivo con retransmisión En esta técnica (ver figura 1.61) el receptor confirma mediante un reconocimiento la recepción de los datagramas 1,2,3 solicitando al emisor el envío del datagrama 4. Cuando el emisor recibe el requerimiento del datagrama 4, envía los datagramas 4,5,6 y espera a recibir confirmación del receptor, a la vez que arranca un temporizador que le indicará retransmitir en caso de que no se haya recibido confirmación del receptor en un tiempo preestablecido. En el caso del ejemplo el receptor solicita reenvío del datagrama 5 a lo que el emisor responde. Una vez recibido correctamente el datagrama 5, el receptor solicita el envío del datagrama 7, a lo que el transmisor responde con el envío de los datagramas 7, 8, 9 y así sucesivamente.

B. El nivel sesión OSI

La capa sesión establece, administra y termina las sesiones entre aplicaciones. En esencia la capa sesión coordina los requerimientos y respuestas de servicio que ocurren cuando las aplicaciones se comunican entre diferentes *hosts*. Este nivel por lo general ayuda a los niveles superiores a identificar y conectarse a los servicios de red.

El nivel sesión utiliza la información de dirección lógica que proporcionan los niveles inferiores para identificar nombres de servidor y direcciones que necesitan los niveles superiores. Este nivel además se encarga de efectuar "llamadas" e iniciar conversaciones entre dispositivos.

Fundamentalmente realiza dos funciones:

1. Control de diálogo
2. Administración de sesión

B.1 Control de diálogo

El control de diálogo define la dirección del flujo de datos. La dirección del flujo de datos puede ser:

- Simplex o unidireccional
- Semidúplex
- Full dúplex

B.2 Administración de sesión

Se encarga fundamentalmente de establecer, mantener y terminar comunicaciones. A partir de esto, se pueden definir tres tareas en el nivel sesión como administrador:

- Establecimiento de conexión
- Transferencia de datos
- Liberación de la conexión

Establecimiento de conexión. Tiene las siguientes subtareas:

- Verificación de nombres y contraseñas
- Establece números de identificación de conexión
- Acuerda los servicios que se requieren y durante qué tiempo
- Determina el dispositivo que inicia la conversación
- Coordina la numeración del reconocimiento y procedimientos de retransmisión

Transferencia de datos. Tiene las siguientes subtareas:

- Transferencia real de datos
- Confirmación positiva y confirmación negativa
- Reanudar comunicaciones que se interrumpen

Liberación de conexión. Los dispositivos extremos reconocen la pérdida de conexión cuando no reciben reconocimiento positivo o negativo. El solicitante

de servicio reconstruye la sesión y reinicia las comunicaciones usando una sesión nueva.

C. El nivel presentación OSI

La capa presentación realiza en esencia dos funciones: Traducción y Codificación. La traducción se da entre múltiples formatos de representación de datos, si es necesario. Por su lado, la codificación garantiza que las aplicaciones tengan información completamente entendible para procesar.

C.1 Traducción

Para que los computadores digitales puedan ser utilizados, los caracteres y números que entienden las personas, deben ser organizados en series de unos (1) y ceros (0). Para este propósito, los fabricantes de computadoras no han logrado ponerse de acuerdo en el número y los bits que se utilizarán para dicha representación. A más del número de bits, es importante que se tome en cuenta el número de bytes acordados para la producción de datos. Los computadores además, deben estar en la capacidad de presentar datos en los diferentes tipos de caracteres de lenguajes humanos. Por último, debido a que las redes de computadores modernos son heterogéneas, se han incorporado una multitud de sistemas operativos locales y de red, y cada uno de éstos puede utilizar una sintaxis o formato de archivos distintos.

La traducción utiliza fundamentalmente cuatro técnicas para realizar su función:

1. **Traducción de orden de bits.** Determina el número de bits que utiliza cada carácter y el orden en que se deben contar los bits (determina cuál es el bit más y el menos significativo).
2. **Traducción de orden de bytes.** Determinan el orden y el número de bytes agrupados que representan datos. Por ejemplo Intel utiliza el método del "pequeño endian" (el bit menos significativo aparece en primer lugar) para la representación de números complejos, mientras que Motorola utiliza el método del "gran endian" (el bit más significativo aparece en primer lugar).
3. **Traducción de código de caracteres.** El nivel de presentación puede no ser capaz de traducir de un lenguaje a otro, sin embargo es importante que se tenga en cuenta el lenguaje. Debe notarse que el nivel de presentación con traducción a este nivel, se encargará de traducir de un código de caracteres a otro (de ASCII a EBCDIC por ejemplo), considerando que dentro un mismo idioma puede presentarse diferentes códigos de caracteres. Esto se consigue por lo general con el paso directo de un código a otro, o utilizando un tercer código intermedio a ambos mutuamente acordado.
4. **Traducción de sintaxis de archivos.** Debido a que muchos sistemas operativos utilizan diferentes sistemas de archivos, la capa presentación con traducción a este nivel, se encarga de extraer los datos y características de los archivos a partir de un sistema de archivos, y convertirlo en otro sistema de archivos de la red.

C.2 Codificación

La codificación se utiliza principalmente para mantener información privada, fuera del alcance de personas ajenas. Para cumplir con este propósito, se utilizan diferentes técnicas de codificación, entre ellas:

1. Transposición
2. Substitución
3. Algebraico

Para que el receptor pueda entender los datos, deberá contar con una unidad decodificadora que utilice el mismo algoritmo que utilizó el codificador en el transmisor. La codificación y decodificación puede realizarse mediante procesos de *hardware* y *software*, pero entre extremos es más común utilizar codificación por *software*.

Para notificar a las entidades el método de codificación que se está utilizando, se utilizan dos tipos de claves:

a. **Claves privadas.** Las entidades que poseen esa clave pueden codificar y decodificar todos los mensajes. Es importante que la clave sea guardada en un lugar seguro.
b. **Claves públicas.** Las "entidades clientes" interesadas, reciben una clave secreta y un valor conocido. Una "entidad distribuidora" crea un clave pública mediante el valor de la clave secreta y el valor conocido. La "entidad distribuidora" inicia la comunicación enviando su clave pública al o los receptores. La "entidad cliente" recibe la clave pública y la combina matemáticamente con su clave secreta para obtener el valor de codificación mutuamente acordable. Debido a que los algoritmos utilizados por lo general son muy complejos, aún teniendo la clave pública y la clave secreta, sería muy demoroso el decifrar el valor de codificación en un tiempo razonable.

D. El nivel aplicación OSI

El nivel aplicación del modelo de referencia OSI, orienta a que los protocolos relacionados con este nivel, puedan brindar los servicios de red, anunciarlos y permitir su uso.

D.1 Servicios de red

Dentro de los servicios de red pueden numerarse los siguientes:

- Servicios de archivos
- Servicios de impresión
- Servicios de mensajes
- Servicios de aplicaciones
- Servicios de base de datos

- Servicios especializados

D.2 Anuncio de servicios

Los servidores anuncian a los clientes los tipos de servicios que proporcionan (notificación de servicios). Se utilizan dos tipos de notificación de servicios:

1. **Notificación activa.** El servidor o notificador de servicios envía mensajes periódicos (incluyendo direcciones del servidor -direccionamiento de servicios) para anunciarse incluyendo por lo general un tiempo de validez de su anuncio de servicio.
2. **Notificación pasiva.** Los proveedores de servicios tienen anotados sus servicios y dirección en un directorio, y cuando un cliente requiere identificar los servicios que proporciona, accesan a ese directorio.

D.3 Uso de servicios

Para que un servicio de red pueda ser utilizado, éste deberá estar disponible para el sistema operativo local del computador. Esto se consigue con las siguientes técnicas:

1. **Intercepción de llamada del sistema operativo.** En esta técnica, los servicios de red son vistos como locales para el sistema operativo de red local.
2. **Funcionamiento remoto.** El sistema operativo local es consciente de los servicios de red disponibles y es el responsable de acceder a ellos. Sin embargo al servidor la presencia del cliente es transparente.
3. **Colaborativo.** Tanto el servidor como el cliente son conscientes de su existencia y trabajan en conjunto para el uso de determinado servicio.

1.3 RED ESTRUCTURADA DE DATOS

La historia de la humanidad se ha caracterizado por ir implementando sistemas que cada vez son más organizados. La experiencia nos dice que es preferible dedicar más tiempo a la planificación que a la remodelación. Hablar de sistemas estructurados, es en general hablar de sistemas organizados, los cuales se caracterizarán por su flexibilidad, confiabilidad, modularidad, facilidad de integración (cumplimiento de estándares) y sencillez. Por las características que poseen los sistemas estructurados, las ventajas son evidentes en cuanto a ahorro de tiempo, esfuerzo y dinero.

Dentro de las redes de datos, la evolución hacia sistemas estructurados no podía dejarse de lado. Es evidente que este es el campo en donde más notoria es la necesidad de mantener un sistema estructurado.

Entonces, una red estructurada de datos será aquella que posea todas las características de un sistema estructurado: flexibilidad, confiabilidad, modularidad, compatibilidad con estándares, en resumen, una red segura, productiva y fácil de administrar.

Hasta hace una década aproximadamente (antes de 1984), el crecimiento de las redes era desordenado[10]. Lo que caracterizaba a este crecimiento era lo siguiente:

- Se cableaba después de la instalación de los equipos
- El tipo de cable dependía del sistema.
- El costo bajo era un objetivo primordial
- No se contaba con estándares en cuanto a *software*, *hardware* y protocolos.
- Cuando se requería una nueva instalación se la incluía al diseño original, y en muchos de los casos no solo que se incluía, sino que era necesario cambiar el diseño original. En otros casos ni siquiera se contaba con un diseño.
- No se contaba con documentación.
- No se disponía de monitoreo y control de la red.
- Se dedicaba grandes cantidades de tiempo a nuevas instalaciones y modificaciones
- Se dedicaba grandes cantidades de tiempo al mantenimiento correctivo

Por el contrario, en la actualidad, si bien aún se tienen limitaciones, las redes de datos deben caracterizarse por lo siguiente:

- Dedicar tiempo suficiente a la planificación y diseño.
- Realizar la instalación de la infraestructura de transporte (en lo posible con control centralizado)
- Mantener estándares en cuanto a infraestructura de transporte
- Realizar instalación de subsistema de interconectividad (en lo posible centralizado)
- Mantener estándares del subsistema de conectividad. En lo posible utilizar un sólo tipo de marca que tenga su reputación y aprobación en empresas de características similares.
- Realizar la instalación de equipos servidores y de estación de trabajo, manteniendo un estándar adecuado.
- Mantener en lo posible *software* garantizado en compatibilidad, si fuera posible, de un único proveedor.
- Realizar monitoreo y control
- Dedicar poco tiempo a las nuevas instalaciones y modificaciones.
- Dedicar tiempo al mantenimiento preventivo
- Dedicar poco tiempo al mantenimiento correctivo

Como se habrá notado, la recomendación actual está orientada a tratar de mantener la compatibilidad de equipos utilizando una estrategia poco práctica: adquirir en lo posible elementos de un único proveedor. Esto rompe totalmente el esquema de un sistema abierto, pero en la actualidad, la experiencia nos dice que es lo recomendable. Sin embargo, debe tenerse claro que el objetivo en el ámbito mundial, es contar con sistemas totalmente abiertos de multiproveedores. Si esto se consiguiera, el proceso

[10] En nuestro medio todavía es común encontrar esto.

general de la implementación de una red estructurada de datos local, idealmente se reduciría a lo siguiente:

- Planificación y diseño
- Instalación de la infraestructura de transporte (podría incluir la implementación de otros servicios ajenos a los datos, como por ejemplo voz, CCTV y control en un único tipo de cable)
- Instalación del subsistema de conectividad
- Instalación de los subsistemas de equipos servidores y de escritorio
- Realizar monitoreo y control
- Realizar mantenimiento preventivo

La experiencia muestra, que con el transcurso del tiempo, resulta más costoso la instalación y mantenimiento de una red tradicional, que la implementación de una red estructurada de datos.

Resulta difícil imaginarse una red que no tenga cambios y crecimiento. Sin embargo, el problema es afrontable desde otro punto de vista: una red estructurada de datos, debe estar preparada para adaptarse fácilmente a cualquier cambio y crecimiento presente y futuro. Una red perfectamente estructurada será aquella que una vez instalada, sea buena por siempre, se adapte a cualquier cambio con un costo bajo, y nunca tenga tiempo sin servicio. Debido a que las situaciones ideales no existen, deben plantearse objetivos que hagan una realidad lo más cercana a lo ideal. Las metas y objetivos cumplirán dos ventajas claves:

- Diseñar alternativas que pueden ser evaluadas versus los objetivos antes de que sean implementados. Los objetivos, proveen una base para comparar una alternativa de implementación con otra. De esta manera, se reduce el riesgo de falsos arranques y sistemas que fallaran ante pequeñas expectativas.
- Los objetivos pueden utilizarse para medir la calidad y rendimiento de la red estructurada una vez instalada. Los objetivos, de esta forma, pueden mostrar las debilidades del sistema y proveer un camino hacia la solución correcta.

Si bien las metas deberán ser establecidas de acuerdo a las expectativas de cada organización, son metas comunes de una red estructurada de datos las siguientes:

- Conectividad: La disponibilidad de conectar cualquier dispositivo de comunicación en cualquier localización.
- Flexibilidad: La facilidad de adaptación a cambios sin detener el funcionamiento normal del resto de la red estructurada.
- Compatibilidad: La habilidad para proveer interoperatibilidad multiproveedor.
- Disponibilidad: La habilidad para proveer los niveles necesarios de tiempo funcional para soportar aplicaciones de misión crítica.
- Capacidad: La habilidad de adaptarse a los requerimientos de crecimiento de la red.

- Productividad: La habilidad de permanecer dentro de las metas de negocios y presupuestos de la empresa.

Debe recordarse finalmente, que el presente trabajo está orientado a redes estructuradas de área local, centrando los mayores esfuerzos hacia los subsistemas de interconectividad e infraestructura de transporte.

Capítulo II

Infraestructura de transporte de una red estructurada de datos, evaluación y administración

II. INFRAESTRUCTURA DE TRANSPORTE DE UNA RED ESTRUCTURADA DE DATOS, EVALUACION Y ADMINISTRACION

2.1 INTRODUCCION

Dentro del sistema de red estructurado propuesto, corresponde tratar el subsistema "infraestructura de transporte".

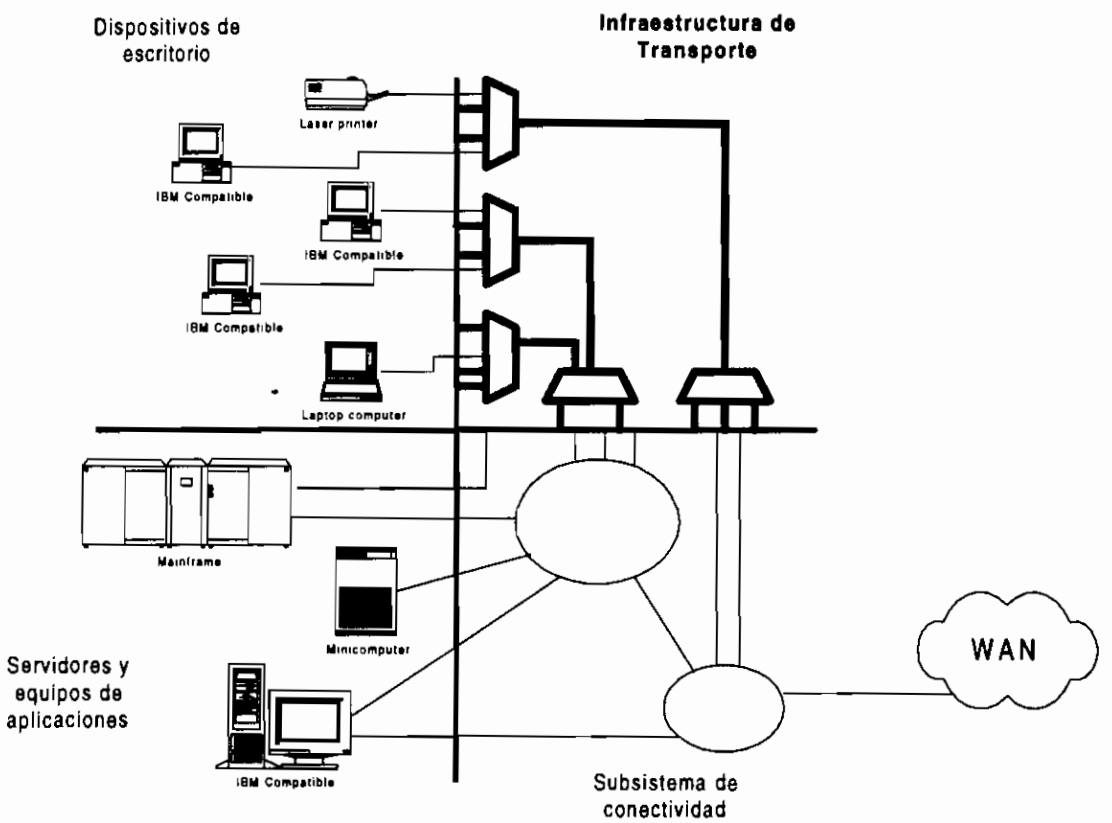


***Figura 2.1** Infraestructura de transporte dentro de una red estructurada de datos*

La infraestructura de transporte debe entenderse como el conjunto de medios físicos que garantizan un camino por medio del cual puede ser transportada la información.

Si bien el término información tiene una definición, en la práctica, este término puede ser relativo a la época. Anteriormente, hablar de transferencia de información podía haber sugerido transmisión de caracteres. En la actualidad, el transporte de información sugiere transmisión de voz, video y datos. De la misma manera en que la información ha ido "creciendo", en la práctica la infraestructura de transporte debe crecer para permitir su transporte.

En general se debería referir a la infraestructura de telecomunicaciones donde estén implícitos el transporte de señales de voz, video, datos, control, *sensing* y señales relacionadas. Sin embargo, como uno de los objetivos de la presente tesis es tratar de dar mayor atención al estudio de los protocolos y dispositivos activos (subsistema de conectividad) encargados del manejo de datos, la tesis ha sido orientada hacia la parte de datos. La extensión de los temas que podrían tratarse (con el presente enfoque) si se considerase el estudio de las redes de telecomunicaciones, sale del marco en tiempo de la presente tesis. Sin embargo, se ha procurado tratar a la infraestructura de transporte de una red estructurada de datos, como una infrestructura de transporte de una red estructurada de telecomunicaciones. Lo mismo es más difícil de realizar cuando se habla del subsistema de conectividad de una red estructurada de datos, principalmente porque tendrían que detallarse equipos orientados a voz y seguridad por ejemplo (según el enfoque de esta tesis).

Por otro lado, la infraestructura de transporte, vista de un modo general, podría ser tan heterogénea como se quisiera, es decir, y como fue en un principio, cada fabricante y cada aplicación podía tener una infraestructura de transporte diferente e incompatible con la de otros proveedores.

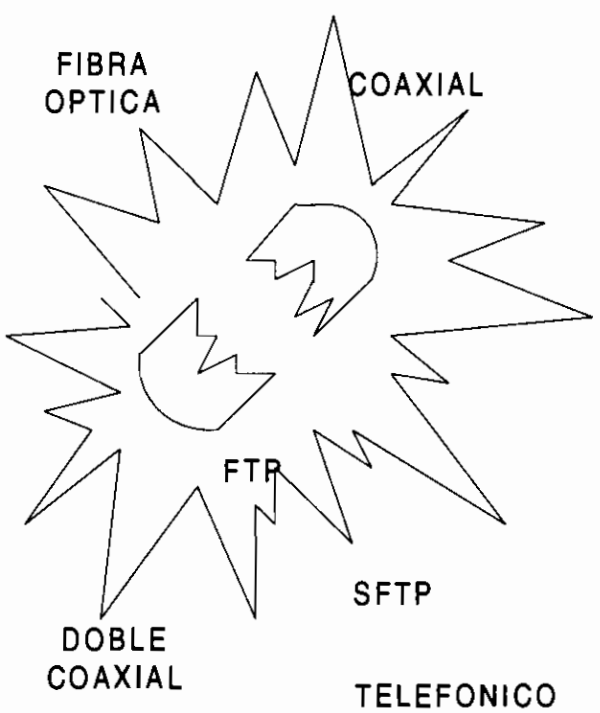


***Figura 2.2** Características de un sistema heterogéneo*

Con el transcurso del tiempo, la proliferación de computadores de escritorio en casi todas las áreas, ha creado la necesidad de confiabilidad, eficiencia y costo efectivo de las comunicaciones.

2.1.1 REQUERIMIENTOS DE USUARIO SOBRE LA INFRAESTRUCTURA DE TRANSPORTE

La comunidad de usuarios, usa la infraestructura de transporte y los dispositivos que se conectan a ella, solamente como un servicio para realizar varias tareas. La infraestructura de transporte se desarrolla a medida que la necesidad de comunicarse con otros dispositivos se vuelve primordial.

Los equipos de usuario, deben ser elegidos no en función de tecnología de punta, sino más bien, en función de los requerimientos que les permitan cumplir bien sus tareas. De esta manera los equipos, computadores y terminales que le resultan útiles a una área, podrían resultar inútiles y obsoletos a otras. Por tal razón, el equipo que se conecta a la infraestructura de transporte, consistirá de una variedad de dispositivos de *hardware* y *software*. Por otro lado, los dispositivos desactualizados que están siendo reemplazados por equipos actualizados, usualmente determinan un período de tiempo en el cual permanecen coexistiendo.

Dentro del ambiente de cambios de dispositivos, se debe añadir las variaciones por crecimiento, disminución y movimiento de grupos de usuarios. Además, las paredes internas de los edificios son cambiadas, los departamentos se mueven de un piso a otro, una área que estuvo formada por un grupo ahora está formada por dos, etc.

Las aplicaciones toman ventaja de la disminución en los costos de *hardware* para proveer más capacidades o presentar una interfaz de usuario más amigable. Anteriormente eran suficientes las páginas llenas de caracteres ASCII, ahora son requeridas páginas con gráficos a color, movimiento y sonido. Estas capacidades añadidas, han determinado que el manejo de bytes ya no sea medido en miles, sino en millones.

La respuesta a todas estas necesidades, es una infraestructura de transporte que responda con eficiencia, confiabilidad y costos razonables a estos cambios.

En resumen, una infraestructura de transporte deberá estar diseñada para responder con eficiencia, confiabilidad y bajo costo a los siguientes requerimientos de la comunidad de usuarios:

- Muchos tipos de dispositivos y protocolos conectados a la infraestrutura de transporte
- La mezcla de dispositivos está continuamente actualizándose
- Las aplicaciones de red multimedia son crecientes
- Los grupos de usuarios están en constante movimiento, crecimiento y disminución.
- Las aplicaciones suelen crecer en versión y en requerimientos.

2.1.2 CARACTERÍSTICAS PRINCIPALES DE LA INFRAESTRUCTURA DE TRANSPORTE[11]

El objetivo principal es tratar de balancear los exigentes requerimientos de la comunidad de usuarios con el diseño de una infraestructura de transporte estable, pero capaz de adaptarse a casi cualquier situación en el presente y futuro.

Como se mencionó en el capítulo anterior, una infraestructura de transporte perfecta, será aquella que una vez instalada es buena por siempre, maneja todos los requerimientos de la comunidad de usuarios productivamente, tiene bajo costo y nunca deja de prestar servicio. Debido a que ésta es una meta ideal, en la práctica se plantean metas y objetivos las cuales son aceptables por la comunidad de usuarios. Las metas necesitan ser tangibles y cuantificables. El trabajar con estas metas y objetivos provee dos ventajas:

- Diseñar alternativas que puedan ser evaluadas contra metas antes de que sean implementadas. Esto reduce el riesgo de que se creen falsas expectativas y que el sistema no responda como debe ante pequeñas fallas.
- Las metas pueden ser usadas para medir la calidad y el rendimiento de la infraestructura de transporte una vez que se ha instalado. De esta forma, también pueden ser utilizadas como guías para corregir cualquier debilidad del sistema.

Además de especificar metas que varían de organización a organización, resulta conveniente definir metas respecto a los siguientes criterios de red:

- Conectividad
- Flexibilidad
- Compatibilidad
- Disponibilidad
- Capacidad
- Modularidad
- Productividad

2.1.3 CRITERIOS DE RED Y OBJETIVOS[12]

2.1.3.1 Conectividad

Es la capacidad de la infraestructura de transporte para asignar a cada una de las salidas (*outlets*) de pared cualquier aplicación actualmente soportada por la empresa.

[11] Tomado de la referencia de cableado estructurado de Ericsson
[12] Según el sistema de cableado Ericsson

La meta de la conectividad debería incluir una medida de la facilidad con la cual se pueden hacer añadiduras, movimientos y cambios en los dispositivos conectados a la infraestructura de transporte. Deberían hacerse las siguientes consideraciones:

- La velocidad con la que pueden realizarse los cambios
- El nivel de personal requerido
- El costo de *hardware* de reemplazo (si se requiere)
- Los sitios donde los servicios pueden ser afectados durante el cambio.

La infraestructura de transporte debería ser independiente de los requerimientos de los departamentos, de tal forma que cualquier salida sea capaz de soportar cualquier servicio y aplicación. Cualquier servicio ofrecido debería ser añadido o cambiado dentro de 30 minutos sin afectar otros servicios.

2.1.3.2 Flexibilidad

La flexibilidad es la capacidad de la infraestructura de transporte de adaptarse a cambios en la organización y/o tecnología.

La infraestructura de transporte debería ser relativamente inmune a los cambios diarios debidos a reajustes organizacionales o tecnológicos, dentro de una actividad normal de la empresa.

La infraestructura de transporte debería tener una arquitectura abierta la cual no excluya nuevos servicios de comunicación con diferentes velocidades y protocolos. La infraestructura de transporte debería estar preparada para soportar tecnología hasta luego de 5 años. Debe considerarse que el cableado estructurado ofrece una inversión garantizada por 15 años.

2.1.3.3 Compatibilidad

La compatibilidad es la capacidad de conseguir interoperatividad multiproveedor. El resultado de la compatibilidad es una infraestructura de transporte que asegura interoperatividad de los dispositivos de usuario conectados. Es importante por tanto crear y respetar estándares mundiales.

2.1.3.4 Disponibilidad

La disponibilidad se refiera a la medida de la probabilidad de que la infraestructura de transporte esté operacional cuando el usuario lo necesite. Para el usuario, el sistema trabaja o no. El sistema incluye computadores,

terminales, servidores, *hosts*, infraestructura de transporte y subsistema de conectividad.

El objetivo de disponibilidad debe ser del 100%. Sin embargo, se ha considerado que el tiempo fuera de servicio de la infraestructura de transporte debería ser de no más de una hora al año en ambientes comerciales normales, y no más de 6 minutos por año en "ambientes de no parada".

2.1.3.5 Capacidad

La capacidad es la medida de la salida (ancho de banda) que la infraestructura de transporte puede manejar. Con el transcurso del tiempo se ve que el requerimiento de mayor capacidad se ha ido incrementando. En la figura 2.3 se muestra el requerimiento de ancho de banda por usuario en Kbps a lo largo de 30 años:

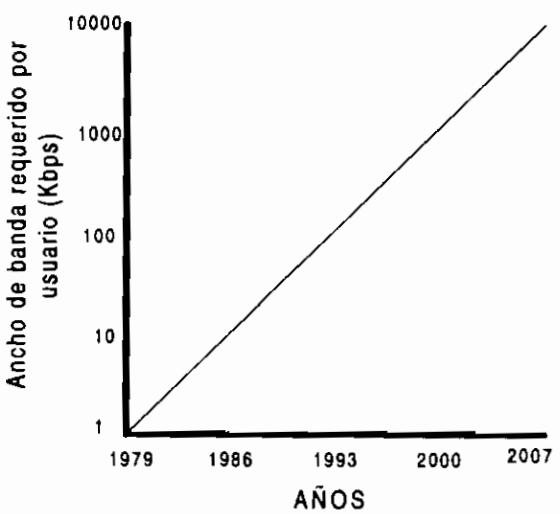


***Figura 2.3** Requerimiento promedio de ancho de banda por usuario en función de años*

En 1979, las comunicaciones de computador consistían de un terminal de caracteres alfanuméricos, y un ancho de banda de 1 Kbps era suficiente para la mayoría de situaciones. En 1986 todavía se mantiene la información envuelta en caracteres ASCII, pero han aparecido los computadores personales y se han incrementado los requerimientos de ancho de banda hasta 10 Kbps. Debido a que se incrementan las aplicaciones, el uso de pantallas gráficas y a color, permite alcanzar un requerimiento de 100 Kbps en 1993, un incremento de 10 veces en 7 años. Los requerimientos actuales de voz, video y datos incrementan la expectativa del ancho de banda, que para el año 2000 será de 1 Mbps por usuario. La gráfica muestra una curva que cumple aproximadamente con la siguiente regla: por cada 7 años, el requerimiento de ancho de banda por usuario se incrementa 10 veces.

Se puede notar que el párrafo anterior hace referencia al uso promedio de ancho de banda de la mayoría de usuarios de sistemas de información en el

mundo. Sin embargo, debe recordarse que actualmente existen aplicaciones gráficas y de multimedia para grupos de usuarios que trabajan simultáneamente y en línea, con procesos que hacen uso de anchos de banda evidentemente mucho más exigentes.

2.1.3.6 Modularidad

La modularidad es la característica que permite ser manejada desde el diseño hasta la implementación, mantenimiento y actualización, y que se encarga de garantizar la maniobrabilidad del sistema en módulos o subsistemas. Es decir, el sistema podrá ser diseñado, implementado, mantenido o actualizado, no necesariamente como un todo, sino por partes. Esto a la larga, se traduce en ahorro de dinero.

2.1.3.7 Productividad

La productividad es una medida del costo versus el beneficio que implica poseer una infraestructura de transporte. Es importante ver que el ser dueño de una buena infraestructura de transporte, es una inversión que se paga sola a mediano plazo. Deben tomarse en cuenta la inversión inicial, versus el costo de los cambios y movimientos en los que se incurriría si no se tuviera una buena infraestructura de transporte. Estudios han mostrado que el 50% de los usuarios están envueltos en cambios y reubicaciones en un período de un año. Se calcula, que en la mayoría de las empresas, el material y los costos de implementar una correcta infraestructura de transporte serían pagados en un período menor a 5 años.

Al costo por cambios y reubicaciones, también debería añadirse la ventaja en dinero que significa tener un sistema con 0 fallos o 100% de disponibilidad, especialmente en empresas donde el tener el servicio disponible es traducido directamente a dinero.

2.2 INFRAESTRUCTURA DE TRANSPORTE DE UNA RED ESTRUCTURADA DE DATOS Y SU RELACION CON EL MODELO OSI

2.2.1 RELACIÓN CON EL MODELO OSI

La infraestructura de transporte está relacionada fundamentalmente con el nivel físico del modelo de referencia OSI, que es el nivel que define las estructuras físicas de la red, las especificaciones mecánicas y eléctricas para la utilización del medio de transmisión, y las normas de codificación y sincronización horaria de la transmisión de bits.

Si se recuerda las partes que integran un subsistema de infraestructura de transporte, se podrá hacer una relación directa con la capa física del modelo OSI en lo referente a definición de estructuras físicas de la red, y de las especificaciones mecánicas y eléctricas del medio de transmisión; sin embargo, no se han considerado normas de codificación y sincronización para transmisión de bits dentro de la infraestructura de transporte. Esto se debe, a que la infraestructura de transporte es la parte "pasiva" de un sistema estructurado de datos, la cual no realiza función activa, sino que permite que sobre ella se monten procesos activos que les corresponderán a los subsistemas de conectividad, y subsistemas de servidores y clientes.

Como se ha mencionado, la infraestructura de transporte es el conjunto de elementos eléctricos y mecánicos que permiten la transmisión de señales electromagnéticas, traducidas en información, y de aquellos que permiten su conexión mecánica. Por tal razón, y como se verá a continuación, cada uno de los elementos que son parte física del sistema de cableado estructurado, están relacionadas con el nivel físico del modelo de referencia OSI.

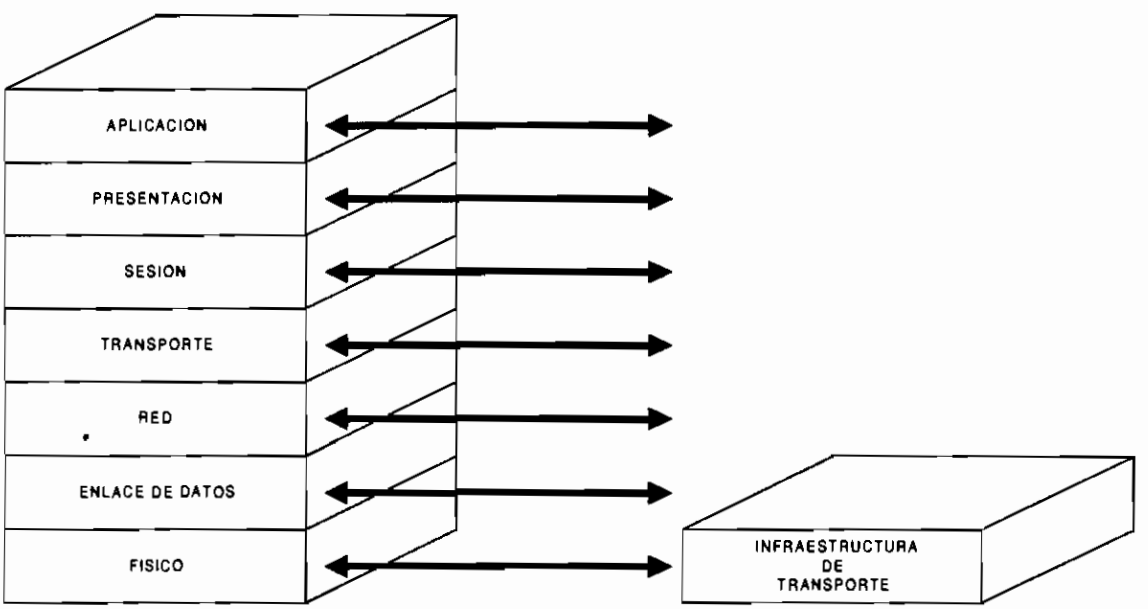


***Figura 2.4** Relación del modelo de referencia OSI y la infraestructura de transporte*

2.2.2 PARTES DE LA INFRAESTRUCTURA DE TRANSPORTE

La infraestructura de transporte está formada fundamentalmente por las siguientes partes:

1. Medio de transmisión
    a. Con cable
    b. Sin cable
2. Conectores, uniones, terminales, salidas, baluns y adaptadores.

Las partes anteriores son parte común e indispensable en cualquier infraestructura de transporte de datos, pero los elementos mencionados a continuación, son partes adicionales que conforman una infraestructura de transporte de datos estructurada.

3. Concentradores y distribuidores de cableado
4. Ductos y canaletas
5. Etiquetado y documentación

2.2.2.1 Medios de transmisión

El medio de transmisión es la vía física por la que viajan las ondas electromagnéticas.

Debido a que las ondas electromagnéticas están relacionadas con un espectro de frecuencias, los medios de transmisión utilizados dependen de la frecuencia asociada al tipo de onda electromagnética que transporta.

A. Espectro electromagnético

La asignación aproximada por frecuencias del espectro electromagnético es mostrada en la tabla 2.1.

B. Factores que caracterizan un medio de transmisión [13]

Cada tipo de medio de transmisión posee determinadas características que definen sus ventajas y desventajas. Estas características están regidas por los siguientes factores:

- Factores técnicos

    a. Capacidad de transmisión y ancho de banda
    b. Resistencia de lazo DC
    c. Longitud de enlace
    d. Velocidad de propagación y permitividad relativa
    e. Impedancia (Conductividad)
    f. Atenuación
    g. SNR (*Signal to Noise Ratio*)
    h. BER (*Bit Error Rate*)

- Factores del medio

    a. *Crosstalk*
    b. EMI Inmunidad ante interferencias electromagnéticas

[13] Tomado de Cabling Vision de Alcatel

Frecuencia en Hz 1 3 10 30 100 300	Líneas eléctricas y telefónicas	 Frecuencia extremadamente baja (ELF)
Frecuencia en KHz 1 3 10 30 100 300	Ondas de radio	 Frecuencia de la voz (VF) Frecuencia muy baja (VLF) Frecuencia baja (LF)
Frecuencia en MHz 1 3 10 30 100 300	Ondas de radio	 Frecuencia media (MF) Frecuencia alta (HF) Frecuencia muy alta (VHF)
Frecuencia en GHz 1 3 10 30 100 300	Microondas	 Frecuencia ultra alta (UHF) Frecuencia super alta (SHF) Frecuencia extremadamente alta (EHF)
Frecuencia en THz 1 3 10 30	Infrarojos	 Ondas submilimétricas Infrarojos lejanos Infrarojos intermedios
Energía de fotones en eV 1 10 100	Ultravioleta	Infrarojos cercanos Espectro visible Ultravioletas cercanos Ultravioletas en el vacío
Energía de fotones en KeV 1 10 100	Rayos X	 Rayos X de baja energía Rayos X de alta energía Rayos gamma de baja energía
Energía de fotones en MeV 1 10 100 1000 10000	Rayos gamma	 Rayos gamma de alta energía Rayos cósmicos secundarios (rayos gamma producidos por rayos cósmicos)

Tabla 2.1 Espectro electromagnético

c. *Jitter*

- Factores secundarios

  a. Costo
  b. Facilidad de instalación

B.1 Factores Técnicos

B.1.a Capacidad de transmisión y ancho de banda

Se ha determinado que la velocidad de una señal (en baudios) viene dada por:

$$V_s = 2\ AB$$

La relación que determina la velocidad de transmisión de datos (en bps) con el ancho de banda requerido por la señal, viene dado por:

$$V_t = 2 * AB * \log_2 (M)$$

y

$$M = 2^n \text{ (en códigos binarios)}$$

donde:

V_t = Velocidad de transmisión (bps)
AB = Ancho de banda requerido por la señal (Hz)
M = número de símbolos
n = Número de bits transmitidos simultáneamente por símbolo

La relación mencionada fue desarrollada por Harry Nyquist (1889-1967), cuyo modelo matemático muestra claramente que en la ausencia de ruido, la capacidad de transmisión se incrementa cuando se utilizan dibits, tribits, etc. Sin embargo, en condiciones reales, esto no es tan cierto. Claude Shannon, un científico de Bell Labs, desarrolló un teorema que incluye el efecto del ruido para mostrar la capacidad de transmisión de un canal (en bps):

$$C = AB * \log_2 (1 + SNR)$$

donde:

C = Capacidad de transmisión de un canal (bps)
SNR = Relación señal a ruido

Es importante observar que el ruido es una variable incluida por el canal, mas no una característica de la señal de datos.

Por ejemplo, para transmitir 155 Mbps sobre un canal de 30 MHz, requiere un mínimo de 35 dB de relación señal a ruido.

B.1.b Resistencia de lazo DC

Todos los conductores insertan una cierta resistencia DC dentro de un circuito. Esta resistencia consume una parte de la energía de la señal conducida y la disipa como calor. Mientras más alta sea la resistencia, más alta será la energía absorbida, produciendo problemas en la transmisión.

Para la medición de este parámetro tan solo es necesario un óhmetro para medir el un extremo del medio, mientras el otro permanece cortocircuitado.

B.1.c Longitud de enlace

Las topologías LAN imponen una longitud de enlace máxima (ejemplo: 10base2 < 185 m, 10baseT < 100 m). Esta limitación es calculada como una función de la temporización de la red (ejemplo: espera de retransmisión) y la máxima tasa de bits erróneos (BER) aceptada. Esto significa que si el enlace es muy grande, el tiempo de transmisión podría exceder la espera máxima especificada por la aplicación.

La degradación de la señal (atenuación) a lo largo del enlace es también un factor limitante a la máxima distancia entre el equipo activo y la estación.

Una técnica utilizada actualmente para medir la longitud de los cables es conocida como TDR (Time Domain Reflectometry). Este método consiste en enviar una señal a través de un cable cortocircuitado en el otro extremo. Una vez que se recibe la señal reflejada, se calcula el tiempo que se demoró en ir y volver la señal. En consecuencia, es muy importante conocer la velocidad de propagación como especificación del cable. Actualmente, los probadores de cable utilizan la velocidad nominal de propagación:

$$L = \Delta t * (VP/2)$$

donde:

L = longitud del enlace
Δt = tiempo de espera entre el envío y recepción de la señal
VP = velocidad de propagación de la señal a través del conductor

B.1.d Velocidad nominal de propagación (NVP) y permitividad relativa

Debido a que la velocidad de propagación para un medio determinado es generalmente un número difícil de recordar (ej. 217.800 Km/s para UTP), se definió la velocidad nominal de propagación (NVP).

La velocidad nominal de propagación se define como la razón en porcentaje entre la velocidad de propagación del medio a prueba, y la velocidad de propagación máxima de la luz en el vacío (300000 Km/s).

$$NVP = (VP / C) * 100\ \%$$

Para el mismo caso de UTP por ejemplo, se habla de 66% de NVP.

Con un error programado del 15% en un instrumento probador, se mide el NVP de un cable utilizando la técnica TDR. Usualmente se toma como longitud de medida del cable prueba como 100 m. NVP será calculado por el instrumento probador en base a la siguiente relación:

$$NVP = (2 * l) / (\Delta t * C)$$

donde:

l = longitud de la muestra de cable
Δt = tiempo de espera entre el envío y recepción de la señal
C = velocidad de la luz en el vacío

También se establece una relación entre la velocidad nominal de propagación y la permitividad relativa:

$$NVP = 1 / \sqrt{\varepsilon_r}$$

donde:

ε_r = permitividad relativa

con:

$$\varepsilon_r \geq 1 \quad y \quad 0 \leq NVP \leq 1$$

B.1.e Impedancia característica

La impedancia característica es frecuentemente confundida con la resistencia DC debido a que ambas suelen expresarse en ohmios. Sin embargo, se debe recordar que la impedancia considera resistencias, capacitancias e inductancias del cable, sobre un determinado rango de frecuencias.

La impedancia característica es función de la distancia entre los dos alambres de un par, y de las características eléctricas de aislamiento.

$$Z_o = (1 / \sqrt{\varepsilon_r}) * f_{(D/d)}$$
$$Z_o = NVP * f_{(D/d)}$$

donde:

Z_o = Impedancia característica
ε_r = Permitividad relativa
D = Distancia entre dos alambres de un par
d = diámetro de un alambre del par
$f_{(D/d)}$ = Función de la relación D/d

B.1.f Atenuación

La atenuación es el debilitamiento de la señal conforme se aleja del punto de origen. Esto significa que entre la atenuación y la distancia, existe una relación lineal. La atenuación generalmente se expresa en decibelios por cada 100 metros (dB/100m). Este es el principal factor a considerarse en el diseño de una LAN.

$$\alpha \approx R / (2 * Z_o)$$

donde:

α = atenuación
R = Resistencia del circuito a una frecuencia considerada
Z_o= Impedancia característica

Lo recomendable es buscar una alta característica de impedancia, y una baja atenuación, con el menor diámetro posible en el cable.

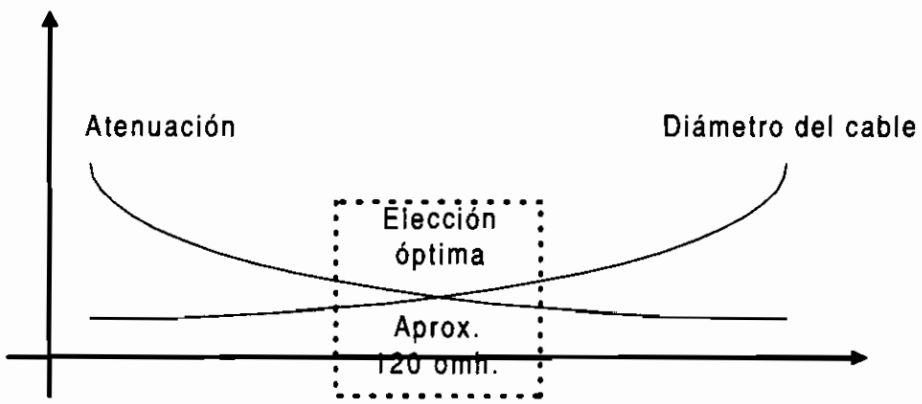


***Figura 2.5** Selección óptima de impedancia*

B.1.g Relación señal a ruido (SNR-*Signal to Noise Ratio*)

La relación señal a ruido, como su nombre lo dice, es la relación establecida entre una señal entrante, contra el ruido que existe sobre ella, medidos en un mismo rango de frecuencias. Esencialmente la relación se establece entre la amplitud más grande de señal, versus la amplitud más grande de ruido que ésta contiene.

Para la mayoría de sistemas, al menos 10 dB de SNR son necesarios para una operación de mínimo error. En esos sistemas, SNR es directamente relacionado con el BER. Se debe notar que una mayor relación señal a ruido SNR, indica un mayor nivel de inmunidad al ruido.

B.1.h BER (*Bit Error Rate*)

Se define como la relación entre el número de bits de un mensaje recibidos con error y el número total de bits transmitidos en ese mensaje. Es una medida de la calidad de transmisión de datos usualmente expresada como un número referido a una potencia de 10. (Ej: un BER de 10^{-3} significa que se produce 1 bit erróneo por cada 1000 bits transmitidos).

B.2 Factores del medio

B.2.a *Crosstalk* (XT)

Se conoce como *crosstalk* a la energía no deseada que se transfiere desde un circuito o alambre a otro, el cual interfiere con la señal deseada. Usualmente es causada por inductancia excesiva en un circuito.

Debido a que una gran cantidad de sistemas utilizan un par para transmisión y uno para recepción, se ha definido el término NEXT (*Near Crosstalk*) que representa la mayor y más importante parte del *crosstalk* (XT), y el término FEXT (*Far End Crosstalk*) que es una parte menos significativa del *crosstalk*.

El NEXT es la energía no deseada que se filtra en el canal vecino, pero medida en el origen del canal transmisor, mientras que FEXT es la energía inducida en el canal vecino pero medida en el extremo lejano del origen de la transmisión. Debido a que la señal de FEXT es atenuada en el trayecto, es mucho menos significativa.

Se debe aclarar que el fenómeno de *crosstalk* no es considerado únicamente al inicio o al final del enlace, sino a lo largo de todo el enlace. Por esta razón, es importante considerar que una prueba de *crosstalk* de un medio debería realizarse a lo largo del medio. Debido a que en la práctica la mayoría de probadores hacen un senso del NEXT a lo largo de aproximadamente 40 m, para distancias mayores, las salidas (donde se encuentran las salidas) podrían tener mucha señal inducida no deseada. Para evitar esto, es conveniente que la prueba de *crosstalk* se la realice desde los dos extremos del medio.

Lo mencionado hasta aquí se ha referido a transmisión/recepción de datos utilizando un medio de dos pares de cables (4 hilos). Si se considera la posibilidad real de tener más de 2 pares en un mismo cable (48 pares por ejemplo), el efecto de *crosstalk* se multiplica, debido a que cada par genera *crosstalk* sobre cada uno de los otros pares (47 para el caso del ejemplo). Para solucionar este problema, lo que se puede utilizar es el apantallamiento de cada uno de los pares dentro del cable.

B.2.b Inmunidad ante interferencias electromagnéticas (EMI)

Las interferencias electromagnéticas, también conocidas como ruido, son generadas principalmente por dos fuentes: eléctricas y magnéticas. Este fenómeno es importante considerar en transmisión de datos, debido a las frecuencias con las que se trabaja.

Debido a que las interferencias electromagnéticas pueden provenir de fuentes divergentes, no existe una solución que elimine todas las fuentes de radiaciones electromagnéticas. Sin embargo, deben hacerse consideraciones en la instalación del medio de transmisión y consideraciones de elección de un medio de transmisión adecuado, dependiendo del ambiente de trabajo en el que estará dicho medio.

Dentro de las consideraciones de instalación, es importante identificar el lugar de ubicación de las posibles fuentes de interferencia electromagnética, para evitar la instalación del medio de transmisión cercana a estas fuentes. Son ejemplos de fuentes de ruido las siguientes:

Alta frecuencia:

- CB
- Radio
- Televisión
- Walkie-Talkie
- Teléfono celular
- Equipo de emisión (emisoras)

Frecuencias medias:

- Copiadoras
- Computadores
- Impresoras láser
- Equipo médico
- Máquinas industriales

Baja frecuencia:

- Líneas AC
- Intercom
- Teléfono
- Motores
- Equipos de elevador
- Tiristores, Triacs.

Técnicas para incrementar inmunidad a interferencias electromagnéticas

Para disminuir la influencia de radiaciones electromagnéticas sobre el medio de transmisión de datos, se utilizan varias técnicas entre las cuales se mencionan las siguientes:

- Par trenzado
- Blindaje o apantallamiento

a. Par trenzado

La teoría que justifica que el trenzado de pares (*twisted pair*) genera inmunidad a interferencias electromagnéticas, se explica en la figura 2.6.

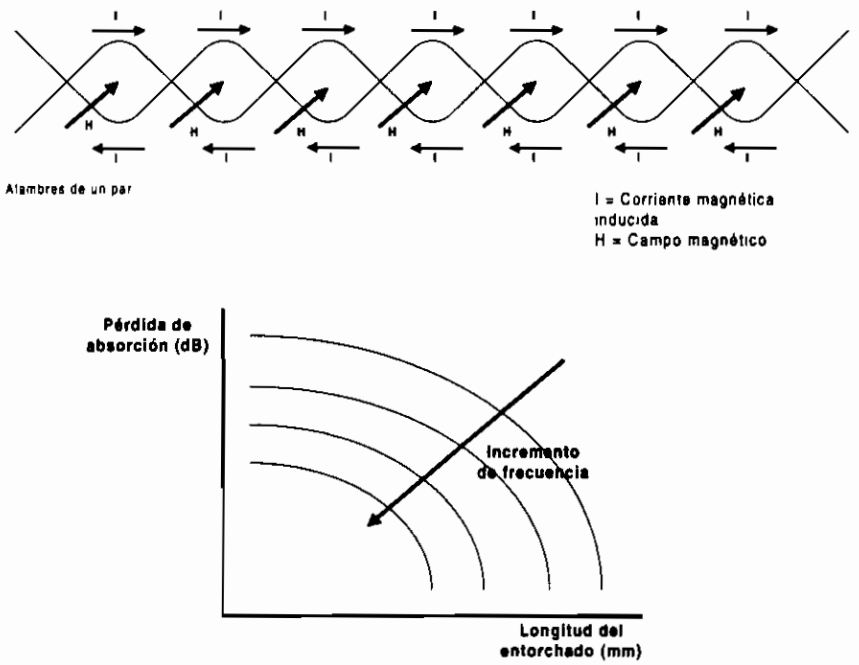


***Figura 2.6** Efecto del par trenzado sobre los campos inducidos*

El campo magnético induce una corriente I_1 en uno de los cables del par, y una corriente I_2 en el otro cable del par. Si la longitud del trenzado es muy pequeña comparada con la longitud de onda del campo magnético, se puede considerar que $I_1 = - I_2$. El efecto del campo magnético en el par trenzado es neutralizado. Pero la longitud del trenzado está mecánicamente restringida a un longitud mínima. Esto significa que para longitudes de onda más pequeñas (frecuencias más altas) la efectividad del trenzado decrementa. Esta técnica es útil cuando se trabaja en rangos de frecuencia que van hasta los 30 ó 40 MHz.

b. Blindaje o apantallamiento

Para EMI con frecuencias sobre los 10 MHz (incluyendo las que sobrepasan los 30 y 40 MHz), es útil la utilización de blindaje sobre el cable de transmisión de datos. La eficiencia del blindaje depende de tres factores:

- Pérdida de reflexión
- Pérdida de reflexión múltiple

- Pérdida de absorción

El primer factor es relativo a la reflexión de una parte de la onda EMI incidente sobre la superficie (hacia afuera) del blindaje. Una parte de la onda penetra dentro del blindaje y es reflejado dentro de aquel, y gradualmente pierde potencia por absorción. Una última parte es simplemente absorbida en el blindaje. La pérdida de absorción es relacionada directamente a las propiedades del material del blindaje, la frecuencia de la onda incidente y el espesor del blindaje. Mientras más grueso el espesor, la absorción mejora. Esto no implica que para todo el rango de frecuencias es mejor utilizar blindaje grueso, pues para frecuencias sobre los 10 MHz se suelen utilizar blindajes muy delgados (en el orden de μm). Esto es debido al efecto skin[14] o efecto piel.

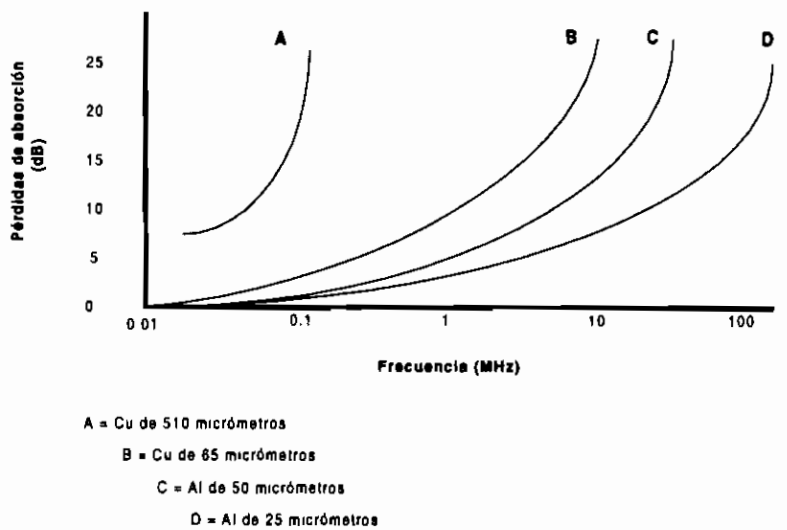


***Figura 2.7** Pérdida de absorción en función de la frecuencia para diferentes materiales*

Como materiales para blindaje se suelen utilizar: acero, cobre y aluminio. Para la elección del material debe considerarse: la rigidez del cable, facilidad de instalación, conductividad, resistencia a la corrosión, calidad de superficie, restricciones de producción, etc.

B.2.c *Jitter*

El *jitter* se puede definir como una modulación de posición de pulso no deseada. Esto significa que el momento de cambio de un bit detectado por el receptor, puede variar en el tiempo. Esto depende del nivel de decisión del comparador.

[14] El efecto Skin dice que las corrientes de altas frecuencias se concentran sobre la superficie del conductor.

Aparte de la atenuación, NEXT e interferencias electromagnéticas, el *jitter* es otro factor importante que tiene impacto sobre la calidad de transmisión en la red. El fenómeno tiene algunas causas. El *jitter* es más relativo a equipo activo (subsistema de conectividad), debido a que las fuentes primarias del *jitter* son regeneradores y multiplexores. Sin embargo, el cableado también introduce *jitter* en el sistema. Al contrario del *jitter* generado por componentes electrónicos, el *jitter* generado por cable es completamente incontrolable. De esta forma, se vuelve mandatorio elegir un sistema que induce la menor cantidad de *jitter*. Esto se puede conseguir, tratando de reducir al máximo el NEXT y la influencia de ruido externo.

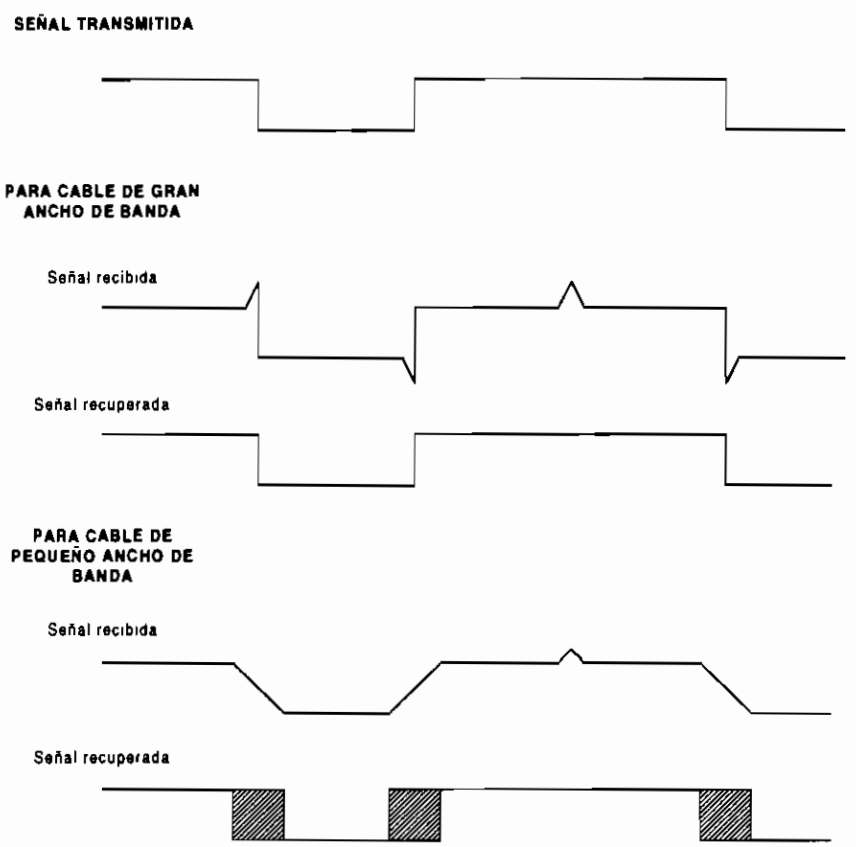


***Figura 2.8** Efecto del jitter sobre una señal digital*

El *jitter* produce que exista una zona gris donde no se puede determinar el estado lógico de la señal. El *jitter* puede ser considerado como ruido en el dominio del tiempo. Claro que el ruido es una modulación de amplitud, la cual es tolerada por el sistema siempre y cuando permanezca dentro de límites bien definidos (relación señal a ruido SNR). De la misma manera, el *jitter* puede tolerarse dentro de ciertos límites, los cuales dependen de que la zona gris deje el suficiente tiempo para conseguir un nivel de detección confiable y haga posible la decodificación.

Un *jitter* muy pronunciado, aumenta el BER y en algunos casos puede llevar a la "caída" del sistema de transmisión de datos. Es muy conocido que la

topología *Token-Ring* es muy sensible al *jitter*. Esto se debe a que la topología en anillo regenera la señal, y los regeneradores son fuentes de *jitter* en equipo activo. La serie de regeneradores origina la acumulación de *jitter*. Inicialmente *Token-Ring* fue diseñado para cable STP, el cual por su blindaje en cada par, disminuía notablemente el NEXT y por tanto el *jitter*. Debido a que el cable UTP es más barato y fácil de instalar, *Token-Ring* se ha venido utilizando sobre UTP. Sin embargo, ha requerido en algunos casos la introducción de filtros pasabandas para disminuir el efecto de NEXT y *jitter*. Ultimamente, el rendimiento que brinda el cable UTP categoría 5, permite que puedan evitarse este tipo de dispositivos.

B.3 Factores secundarios

Se considera como factores secundarios, aquellos factores que por estar fuera de consideraciones técnicas, no deberían influenciar en lo que significa la excelencia de la infraestructura de transporte, pero que en la práctica son factores determinantes en el momento de realizar una elección. Como factores secundarios se consideran los siguientes:

a. Costo relativo
b. Facilidad de instalación

C. Clasificación de los medios de transmisión más utilizados en redes LAN

C.1 Medios de transmisión de cable

Los medios de transmisión de cable, están formados por cables o fibras que conducen la electricidad o la luz. Dentro de los medios de transmisión de cable más conocidos están:

1. Cable de par trenzado
    - No blindado (UTP)
    - Blindado (STP)
        - Foiled (FTP)
        - Screened foiled (S-FTP)
2. Cable coaxial
    - Axial
    - Twinaxial
3. Cable de fibra óptica
    - Unimodal
    - Multimodal

C.1.a Cable de par trenzado

El par trenzado es una disposición utilizada con dos alambres de cobre. La disposición de par trenzado, permite disminuir la influencia de emisiones electromagnéticas y *crosstalk*.

Los alambres de cobre que generalmente se utilizan son 22 AWG o 24 AWG.

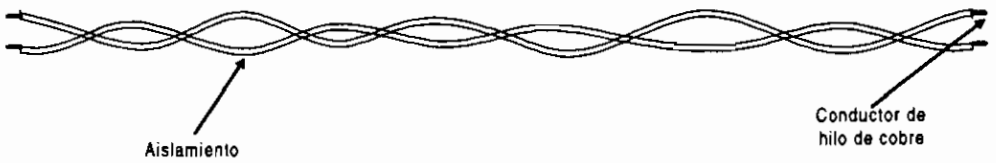


Figura 2.9 Par de hilos trenzados

a. Cable de par trenzado no blindado (UTP)

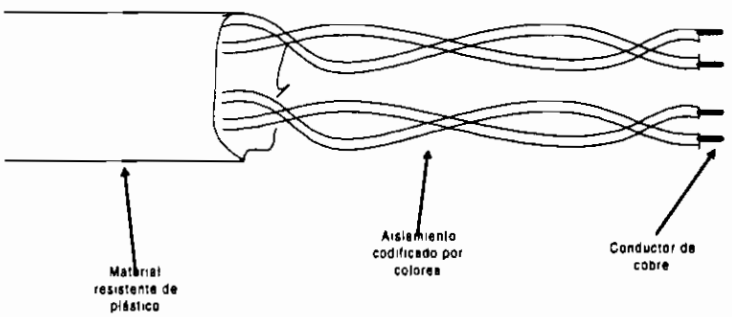


Figura 2.10 Cable UTP

Característica	Cable UTP Categoría 5
Ancho de banda	100 MHz
Capacidad de transmisión	155 Mbps
Resistencia de lazo DC	Aprox. 19.2 Ω
Longitud de enlace	Depende del estándar utilizado: Para 10baseT < 100m
Velocidad de propagación (NVP)	66%
Impedancia (Zo)	Entre 100, 120 y 150 Ω (+/- 15%)
Atenuación	Relativamente elevada
SNR	Con 100 MHz y 155 Mbps se requiere una SNR mínima de 1.92 dB. En la mayoría de sistemas se requiere una relación mínima SNR de 10 dB.
Crosstalk	Susceptible a *crosstalk*
EMI	Susceptible a EMI
Jitter	Susceptible
Costo	Relativamente económico
Facilidad de instalación	Es de fácil instalación, configuración y reconfiguración

Tabla 2.2 Características del cable UTP categoría 5

El cable de par trenzado está formado por un conjunto de pares trenzados, con una única funda de plástico.

Existen cinco categorías de cable UTP, siendo las más difundidas las categorías 3 y 5[15]. La categoría 5 tiene las mejores características.

Los conectores que utiliza este tipo de cable por lo general es el RJ11 (para 2 pares) y el RJ45 (para 4 pares).

b. Cable de par trenzado blindado (STP)

Es un cable que contiene varios pares trenzados pero envueltos por un blindaje metálico, finalmente cubiertos por la funda de plástico.

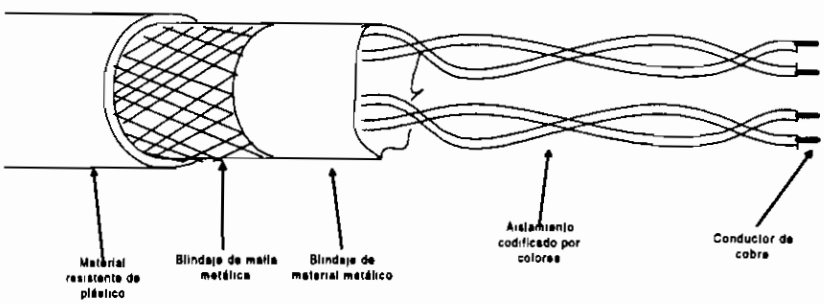


Figura 2.11 Cable STP

Característica	Cable STP
Ancho de banda	Más de 100 MHz
Capacidad de transmisión	500 Mbps (se ha implementado hasta 155 Mbps, y la más utilizada es 16 Mbps)
Longitud de enlace	100 m aproximadamente
Atenuación	Similar a UTP
SNR	Mejor que UTP
Crosstalk	Menos sensible que UTP
EMI	Sensitivo a EMI, pero menos que UTP
Jitter	Susceptible pero menos que UTP
Costo	Más costoso que UTP
Facilidad de instalación	Instalación más complicada que UTP y que coaxial cuando no hay conectores preinstalados. Requiere conexión a tierra del cable.

Tabla 2.3 Características del cable STP

[15] Para una longitud de 100 m de cable, el cable categoría 3 puede soportar aplicaciones clase C (hasta 16 MHz), mientras que el cable categoría 5 puede soportar aplicaciones clase D (hasta 100 MHz) para la misma distancia. Para más información revisar las tablas 2.14 y 2.15 de este capítulo.

b.1 *Foiled Twisted pair* (FTP)

El cable FTP (*Foiled Twisted pair*), trata de mezclar las características técnicas de STP, y las características de manejo de UTP. Está formado por 4 pares trenzados, los cuales están cubiertos por un blindaje de papel metálico (aluminio) y sobre éste la cubierta de plástico muy similar a la del cable UTP.

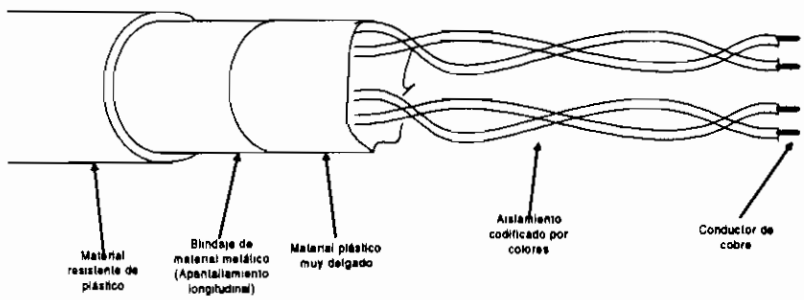


***Figura 2.12** Cable FTP*

Característica	Cable FTP Categoría 5
Ancho de banda	Aproximadamente 100 MHz
Capacidad de transmisión	155 Mbps
Resistencia de lazo DC	Aproximadamente 19.2 Ω
Longitud de enlace	Aproximadamente 90 m.
Velocidad de propagación (NVP)	Aproximadamente 75%
Impedancia (Zo)	Aproximadamente 120 Ω (+/- 15%)
Atenuación	17 dB/100m para cables de 120 Ω 22 dB/100m para cables de 100 Ω
SNR	Con 100 MHz y 155 Mbps se requiere una SNR mínima de 1.92 dB. En la mayoría de sistemas se requiere una relación mínima SNR de 10 dB.
Crosstalk	Menos sensible que UTP y un poco más que STP
EMI	Menos sensible que UTP y un poco más que STP
Costo	Más caro que UTP pero más económico que STP
Facilidad de instalación	Es de fácil instalación, configuración y reconfiguración

***Tabla 2.4** Características del cable FTP*

b.2 *Screened Foiled Twisted pair* (S-FTP)

De las mismas características que el cable FTP, pero adicionalmente contiene una cubierta de blindaje de apantallamiento de malla, que le da mayor resistencia frente a las EMI.

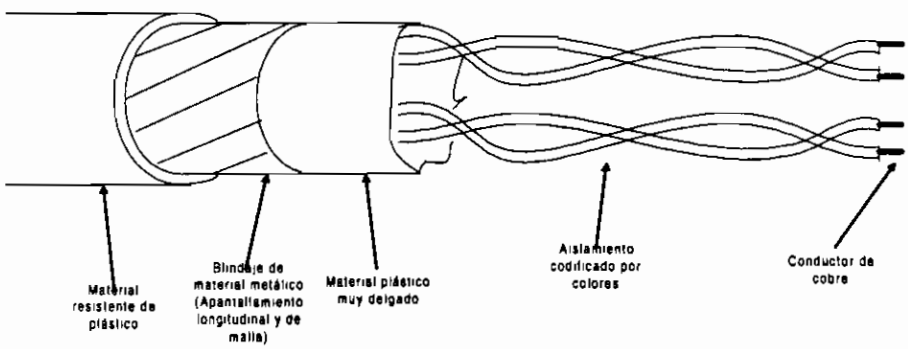


***Figura 2.13** Cable S-FTP*

Característica	Cable S-FTP Categoría 5
Ancho de banda	Aproximadamente 100 MHz
Capacidad de transmisión	155 Mbps
Resistencia de lazo DC	Aproximadamente 19.2 Ω
Longitud de enlace	Aproximadamente 90 m.
Velocidad de propagación (NVP)	Aproximadamente 75%
Impedancia (Zo)	Aproximadamente 120 Ω (+/- 15%)
Atenuación	17 dB/100m para cables de 120 Ω 22 dB/100m para cables de 100 Ω
SNR	Con 100 MHz y 155 Mbps se requiere una SNR mínima de 1.92 dB. En la mayoría de sistemas se requiere una relación mínima SNR de 10 dB.
Crosstalk	Menos sensible que UTP y un poco más que STP
EMI	Menos sensible que UTP y un poco más que STP
Costo	Más caro que UTP pero más económico que STP
Facilidad de instalación	Es de fácil instalación, configuración y reconfiguración

***Tabla 2.5** Características del cable S-FTP*

C.1.b Cable coaxial

a. Axial

Es un cable formado por dos conductores que comparten un eje común. Por lo general el centro del cable es un hilo de cobre relativamente rígido o un hilo acordonado envuelto en un recubrimiento plástico aislante. El recubrimiento está cubierto por un segundo conductor, un tubo de malla de hilo (algunos incluyen una envoltura metálica conductora), que sirve como blindaje frente a las EMI. Finalmente un tubo plástico duro aislante forma la cubierta del cable.

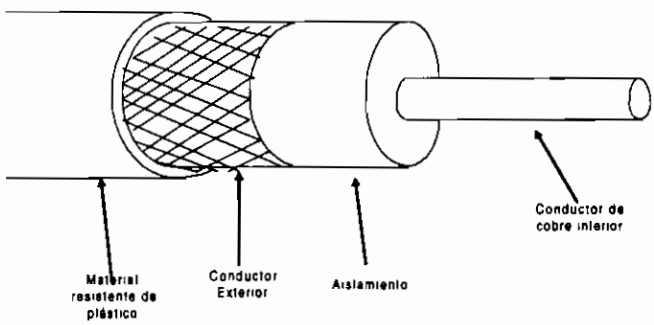


Figura 2.14 Cable coaxial

Característica	Cable coaxial-axial
Capacidad de transmisión	Por lo general se utiliza para transmitir 10 Mbps.
Longitud de enlace	Pocos miles de metros
Atenuación	La señal se atenúa menos que el par trenzado
EMI	Presenta mayor inmunidad a EMI que el par trenzado. El blindaje reduce enormemente el efecto de EMI.
Costo	El costo aumenta con el diámetro y la composición de los conductores. RG-58 es más barato que STP y UTP cat. 5. Pero RG—8 y RG-11 son más caros que STP y UTP cat. 5.
Facilidad de instalación	La instalación inicial es relativamente sencilla, pero es difícil de administrar y reconfigurar.

Tabla 2.6 Características del cable coaxial

Los tipos más habituales de especificaciones de cable coaxial utilizadas como infraestructura de transporte de redes de datos, son los siguientes:

- RG-8 y RG-11 de 50 Ω (utilizadas en Ethernet gruesa)

- RG-58 de 50 Ω (utilizadas en Ethernet delgada)
- RG-59 de 75 Ω (utilizadas en TV por cable)
- RG-62 de 93 Ω (utilizadas en Arcnet)

b. Twinaxial

Es un tipo especial de cable compuesto por un par trenzado, el cual se encuentra compartiendo un eje con una malla metálica y una cubierta de plástico relativamente grueso. Entre el par trenzado y la malla metálica se encuentra un material plástico semirígido.

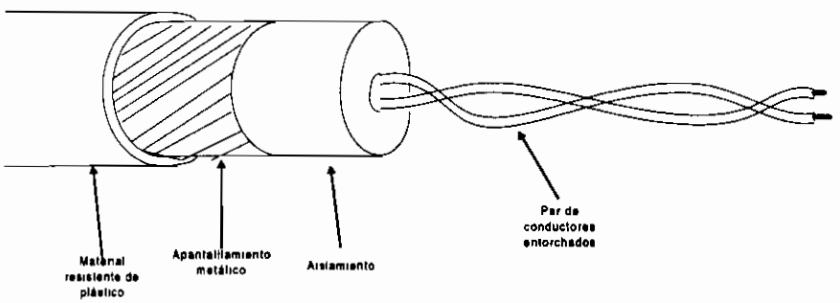


Figura 2.15 Cable twinaxial

Característica	Cable coaxial-twinaxial
Longitud de enlace	Pocos miles de metros
EMI	Presenta mayor inmunidad a EMI que el par trenzado y que el axial. El blindaje reduce enormemente el efecto de EMI.
Costo	Más costoso que el axial
Facilidad de instalación	La instalación inicial es relativamente sencilla, pero es difícil de administrar y reconfigurar.

Tabla 2.7 Características del cable twinaxial

C.1.c Cable de fibra óptica

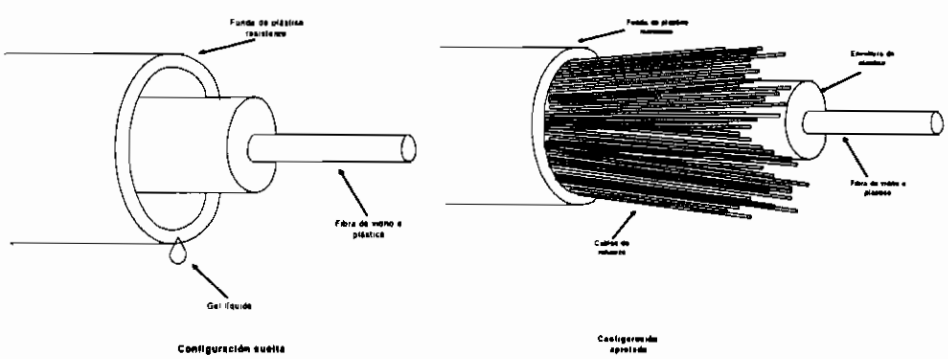


Figura 2.16 Cable de fibra óptica en configuración suelta y configuración apretada

La fibra óptica está formada por un núcleo de vidrio (extremadamente puro[16]) o de plástico conductor de luz, rodeado de más vidrio denominado revestimiento y un forro exterior duro. El núcleo central proporciona el recorrido de la luz o canal de ondas, mientras que el revestimiento está formado por varias capas de vidrio reflector. El revestimiento está diseñado para refractar la luz de nuevo hacia el núcleo. Cada cordón del núcleo y del revestimiento está rodeado por un forro apretado o suelto.

Las configuraciones apretadas tienen el cordón rodeado por cable de refuerzo, mientras que las configuraciones sueltas están rodeadas de un gel líquido. En los dos casos el forro exterior proporciona la dureza necesaria para proteger al cable de variaciones excesivas de temperatura, dobleces, rayones y roturas.

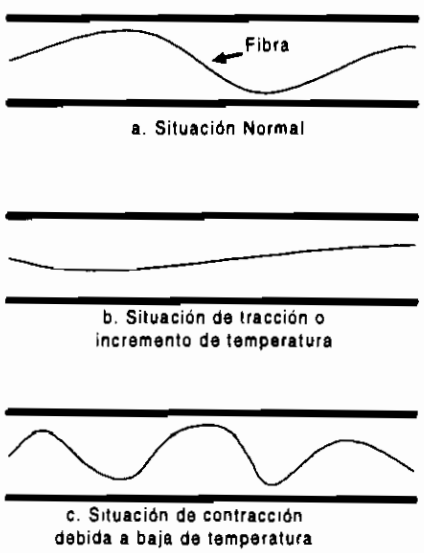


***Figura 2.17** Efecto de la temperatura sobre el cable de fibra óptica*

Para proveer sobrelongitud del tubo, la fibra se suele poner en una disposición helicoidal dentro del mismo.

***Figura 2.18** Disposición helicoidal de la fibra dentro del tubo*

[16] Para dar una idea del grado de pureza, imaginemos la visibilidad a través de un vidrio de 5 Km de ancho.

Debido a que las fibras ópticas son mucho más pequeñas y ligeras que los alambres de cobre, ocupan mucho menos espacio, lo que las hace ideales para aplicaciones con entornos de espacio limitados.

a. Fibra óptica unimodal

La fibra unimodal se ha optimizado para que permita un solo recorrido de la luz. El diámetro del núcleo en la fibra unimodal es aproximadamente de 9 µm.

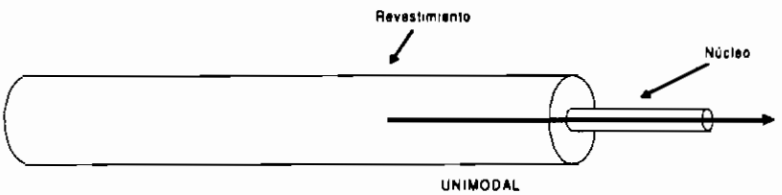


Figura 2.19 Fibra óptica unimodal

El tipo de fibra unimodal más utilizado es con núcleo de 8,3 µm y un revestimiento de 125 µm.

Característica	Cable de fibra óptica unimodal
Capacidad de transmisión	Entre 100 Mbps y 2 Gbps
Velocidad de propagación (NVP)	Aproximadamente la velocidad de la luz
Atenuación	Inferior a 20 dB/Km
Crosstalk	Inmune a *crosstalk*
EMI	Totalmente inmune a EMI
Costo	El más costoso de los medios de cable
Facilidad de instalación	Relativamente complicado de instalar y configurar.

Tabla 2.8 Características del cable del cable de FO unimodo

b. Fibra óptica multimodal

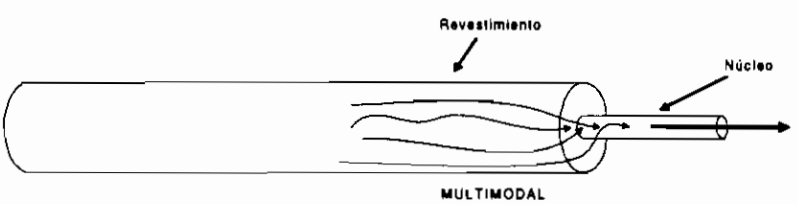


Figura 2.20 Fibra óptica multimodal

La fibra multimodal permite varios recorridos de la luz, refractando la luz a diferentes velocidades, haciendo que las partes lleguen simultáneamente y el receptor las interprete como un único impulso. Debido a esto, presenta menor capacidad que la fibra unimodal, pero es más económica. El diámetro del núcleo de la fibra multimodal está en el orden de las decenas de micrómetros.

Los tipos de fibra multimodal que más se utilizan son: con núcleo de 62,5 µm y revestimiento de 125 µm; con núcleo de 50 µm y revestimiento de 125 µm; y con núcleo de 100 µm y revestimiento de 140 µm.

Característica	Cable de fibra óptica multimodal
Capacidad de transmisión	Entre 100 Mbps y 2 Gbps
Velocidad de propagación (NVP)	Aproximadamente la velocidad de la luz
Atenuación	Inferior a 20 dB/Km
Crosstalk	Inmune a *crosstalk*
EMI	Totalmente inmune a EMI
Costo	Menos costoso que fibra unimodal pero más costoso que los otros medios.
Facilidad de instalación	Relativamente complicado de instalar y configurar.

***Tabla 2.9** Características del cable del cable de FO multimodo*

C.2 Medios de transmisión sin cable

Los medios sin cable transmiten señales electromagnéticas sin utilizar ningún conductor eléctrico u óptico. La atmósfera proporciona el medio físico de transmisión de los datos.

Dentro de los medios sin cable más difundidos se encuentran:

1. Radiofrecuencia (entre los 10 KHz y 1 GHz)
   - Radio unifrecuencia de baja potencia
   - Radio unifrecuencia de alta potencia
   - Radio de amplio espectro
2. Microondas
   - Microondas terrestres (Por lo general 4-6 GHz y 21-23 GHz)
   - Microondas por satélite (Por lo general entre 11y 14 GHz)
3. Infrarojos (entre los 100 GHz y 1000 THz)
   - Punto a punto
   - Difusión

De los sistemas de transmisión de datos sin cable mencionados, los que en la práctica se utilizan para implementaciones LAN son los siguientes:

1. Radio unifrecuencia de baja potencia
2. Microondas terrestres
3. Sistemas infrarojos
   - Punto a punto
   - Difusión

Las razones para que no se utilicen los otros sistemas como infraestructuras de transporte para redes de área local, principalmente son:

- Utilizan bandas de frecuencia reguladas por organizaciones regionales e internacionales, por lo que ocasionan: demoras en la adquisición de licencias y por tanto demoras en la implementación, aumento de los costos y poca flexibilidad para el traslado del equipo.
- Utilizan potencias de transmisión demasiado grandes para una LAN.
- Tecnología demasiado compleja y costosa para una LAN.

C.2.a Radio unifrecuencia de baja potencia

Debe conocerse que el espectro de frecuencias se ha dividido en bandas de frecuencia reguladas y no reguladas. A pesar de que las bandas de frecuencia reguladas garantizan transmisiones claras dentro de un área específica, la obtención del permiso respectivo y el costo que involucran son costosas en tiempo y dinero. Por esta razón, las bandas no reguladas son codiciadas, aunque no garantizan ninguna área de transmisión sin una posible interferencia. Debe conocerse, que si bien las bandas de frecuencia no reguladas permiten la libre utilización de la frecuencia en ese rango, las potencias a las que se puede transmitir si están limitadas, y por lo general no llegan a 1 vatio, justamente para evitar interferencias.

El uso de una única frecuencia con baja potencia, es factible en entornos abiertos y de cortas distancias. Sin embargo, la utilización de frecuencias bajas y potencias bajas, limita las velocidades de transmisión (rangos en el orden de 1 hasta 10 Mbps) y las distancias de alcance (en el orden de los 25 y 30 metros aproximadamente).

Característica	Radio unifrecuencia de baja potencia
Capacidad de transmisión	Entre 1 y 10 Mbps
Longitud de enlace	25 - 30 m.
Atenuación	Relativamente elevada
EMI	Baja inmunidad a EMI
Costo	Moderadamente económicos
Facilidad de instalación	Sencilla si los equipos vienen preconfigurados

Tabla 2.10 Radio unifrecuencia de baja potencia

C.2.b Microondas terrestres

Utilizan antenas parabólicas direccionales. El rango de frecuencia que utilizan está en el rango inferior de los GHz. En redes LAN se suelen utilizar para enlazar redes remotas que están en otros edificios, a los cuales sería más difícil y costoso acceder con cable. En muchos de los casos estas frecuencias están reguladas, por lo que es necesario obtener el permiso respectivo. Se pueden también utilizar las microondas a menor escala

dentro de edificios, utilizando pequeños transmisores que se comunican con concentradores omnidireccionales.

Característica	Microondas terrestres
Capacidad de transmisión	Entre 1 y 10 Mbps
Longitud de enlace	Pueden ser de algunos cientos de metros (para LANs) y de varios kilómetros.
Atenuación	Se atenúan con la lluvia y la niebla. En distancias pequeñas la atenuación no es significativa
EMI	Susceptibles a EMI
Costo	Relativamente elevado, pero puede obtenerse el servicio rentado. Para distancias cortas, los costos pueden abaratarse utilizando frecuencias más altas para utilizar antenas más pequeñas y más baratas.
Facilidad de instalación	Puede ser complicada ya que requieren de línea de vista clara y de permiso para el uso de frecuencia cuando ésta es regulada

Tabla 2.11 Microondas terrestres

C.2.c Sistemas infrarojos

La luz que utilizan los sistemas infrarojos es pura, ocupando un rango limitado de espectro electromagnético (en el rango de 100 GHz y 1000 THz). Las señales de infrarojos no son capaces de atravesar paredes ni objetos opacos, por lo que su señal se la puede receptar directamente o por rebote (pierde aproximadamente la mitad de su potencia). Estos sistemas son útiles en entornos pequeños y libres de obstáculos.

La velocidad de transmisión que alcanzan suelen ser relativamente elevadas.

a. Infrarojos punto a punto

Por la facilidad que brindan para concentrar los haces puros de forma precisa, pueden utilizarse para comunicaciones punto a punto con direccionamiento que requiere cierta precisión (semejantes a controles remotos de televisión y radio). Ver tabla 2.12.

b. Infrarojos de multipunto o difusión

Esta técnica utiliza el haz infrarojo de manera difusa para que cubra una mayor área. De esta forma, los receptores pueden captar las señales en cualquier punto del área efectiva, haciendo que la reconfiguración de la red

dentro del área efectiva no sea problema. Sin embargo, esto significa que la señal podría ser también fácilmente "pirateada" en esa área. Ver tabla 2.13.

Característica	Infrarojo punto a punto
Capacidad de transmisión	Puede estar en el orden de pocos Kbps hasta unos 16 Mbps (a 1 Km)
Longitud de enlace	Entre varios metros y pocos kilómetros
Velocidad de propagación (NVP)	Aproximadamente la velocidad de la luz
Atenuación	Depende de la intensidad de la señal, de su pureza y de las condiciones atmosféricas.
EMI	Son susceptibles en condiciones de luz muy intensa.
Costo	Depende del equipo de filtrado que se utilice. Equipos láser de calidad y potencia pueden ser muy costosos. Los equipos que se utilizan generalmente para transmisión de datos son económicos.
Facilidad de instalación	Requieren instalación y mantenimiento para garantizar alineación precisa.

***Tabla 2.12** Infrarojo punto a punto*

Característica	Infrarojo de multipunto o difusión
Capacidad de transmisión	Manejan velocidades de transmisión semejantes a 1 Mbps
Longitud de enlace	Entre varias decenas de metros
Velocidad de propagación (NVP)	Aproximadamente la velocidad de la luz
Atenuación	Depende de la intensidad de la señal, de su pureza y de las condiciones atmosféricas.
EMI	Son susceptibles en condiciones de luz muy intensa.
Costo	Depende del equipo de filtrado que se utilice. Equipos láser de calidad y potencia pueden ser muy costosos. Los equipos que se utilizan generalmente para transmisión de datos son económicos.
Facilidad de instalación	Si se dispone de un ambiente libre de obstáculos, la instalación y reconfiguración es sencilla

***Tabla 2.13** Infrarojo de multipunto o difusión*

2.2.2.2 Conectores, uniones, salidas, baluns y adaptadores

A. Conectores

Los conectores son parte importante de la infraestructura de transporte de cualquier red. Estos dispositivos son diseñados para cada tipo de medio de transmisión de acuerdo a determinadas especificaciones mecánicas y eléctricas, especificadas según estándares. Estos dispositivos están relacionados con el nivel físico del modelo de referencia OSI.

Dentro de los tipos de conectores más utilizados en redes de datos están los siguientes:

1. Conectores coaxiales (BNC)
2. Conector de datos IBM
3. Conector DB-9, DB-15 y DB-25
4. Conectores RJ-45

B. Uniones

Las uniones se encargan de permitir que dos medios de transmisión del mismo tipo permitan extender sus distancias, conservando sus características normales.

C. Terminales y acopladores de impedancia

Los terminales de impedancia cumplen con la función de realizar un acoplamiento de impedancia del cable en sus extremos, con el fin de anular el efecto de señal reflejada por mal acoplamiento. Es frecuentemente utilizado en disposiciones que utilizan cable coaxial con topología física en bus.

Dentro de los terminales de impedancia más conocidos están:

1. Terminales Coaxiales de 50 Ω, 98 Ω
2. Terminales de twinaxial

Los acopladores de impedancia sirven como medio de conexión entre dos medios de transmisión distintos, cuyas impedancias sean distintas.

D. Salidas

Son dispositivos que tienen conectado el medio de transmisión que viene desde los distribuidores, y está disponible en el sitio de trabajo del usuario, para que a él se conecte el equipo de usuario.

2.2.2.3 Concentradores y distribuidores de cableado

Antes de que se presente la necesidad de tener redes estructuradas de datos, la idea de tener un espacio destinado a concentrar todo el cableado y posteriormente redistribuirlo, era utilizada en telefonía solamente. En redes de datos, el cableado llegaba directamente desde el equipo servidor hasta el cliente, y en el mejor de los casos se utilizaba uno varios concentradores que generalmente se ubicaban distribuidos para ahorrar cable.

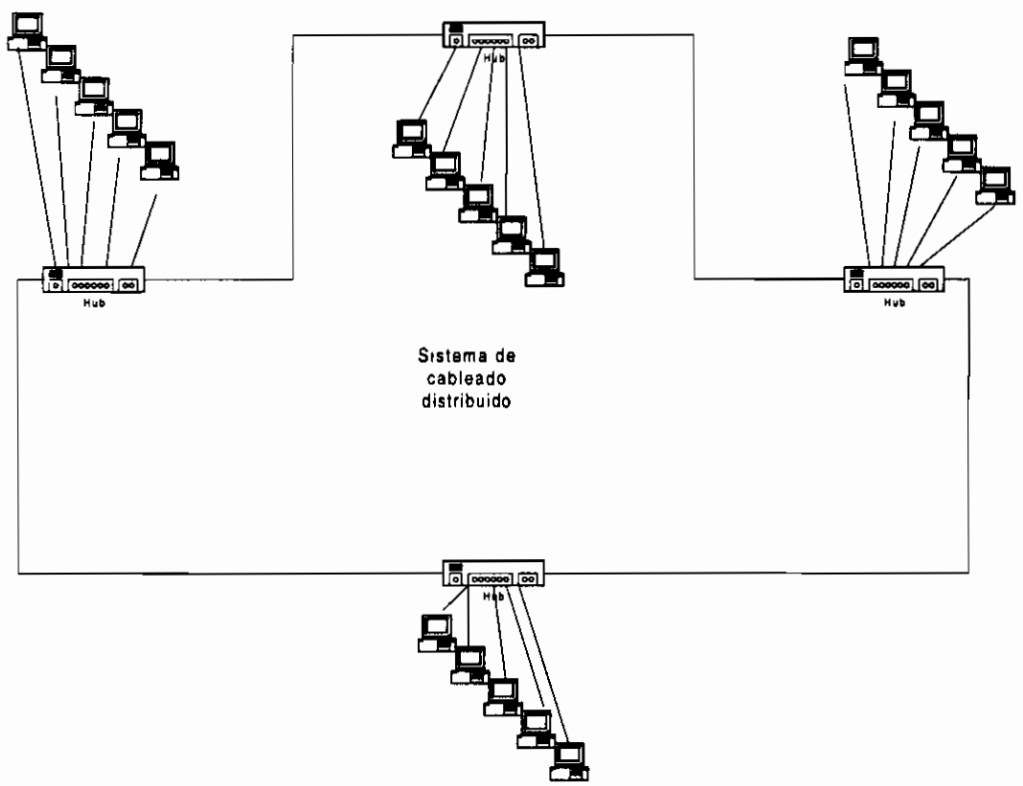


***Figura 2.21** Configuración típica concentradores de una red no estructurada de datos*

Posteriormente, se da más prioridad al servicio y a la facilidad de administración de la red, dejando de lado factores como el ahorro de cable. De esta manera, se destinan espacios donde el cable llega primero a regletas, paneles de distribución ubicados en gabinetes (*racks*), donde se realiza un ordenamiento del cableado que llega. De las salidas de estos centros de concentración y distribución de cableado, se parte hacia los MAU, hubs Ethernet, Arcnet, *Token-Ring*, etc, pasivos o activos que forman parte del subsistema de conectividad.

Debe quedar claro que los concentradores y distribuidores de cableado pertenecientes a la infraestructura de transporte, no cumplen ninguna función de conectividad, sólo

permiten la mejor administración y ordenamiento del cableado. Son dispositivos totalmente pasivos y no realizan ninguna función inteligente.

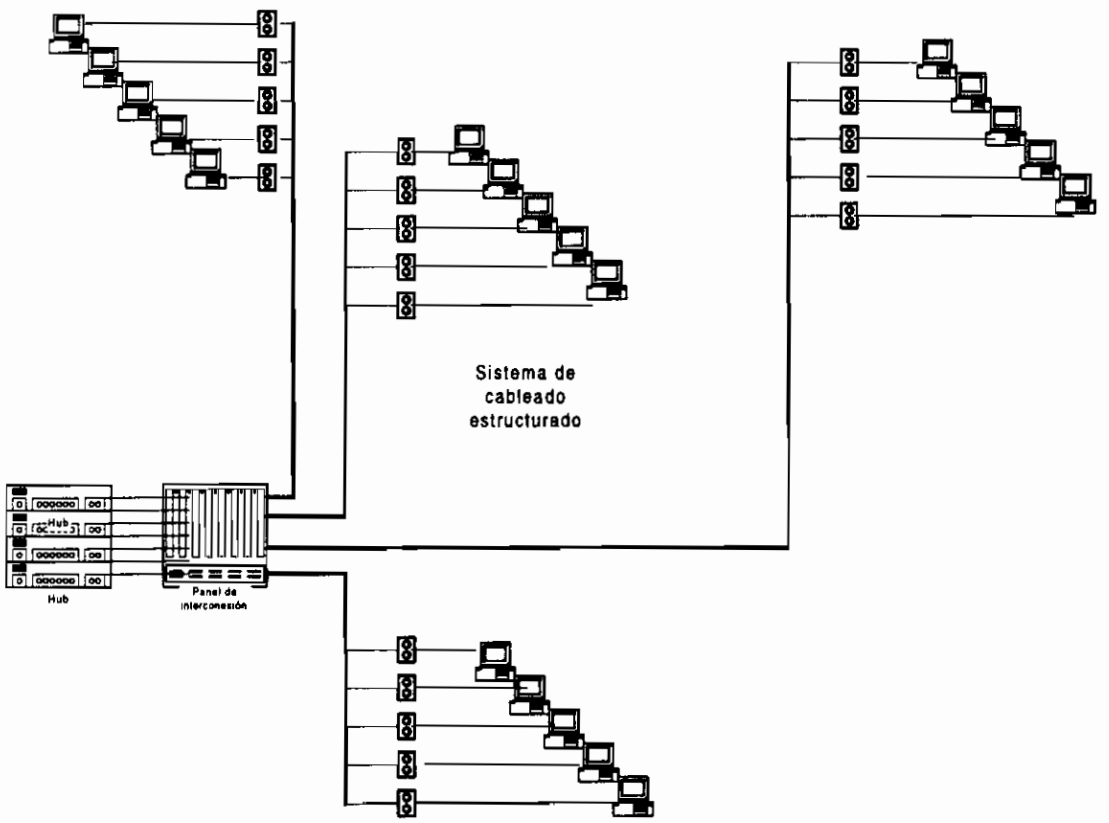


Figura 2.22 Configuración típica de concentradores de una red estructurada de datos

2.2.2.4 Ductos y Canaletas

Es importante que el cable se encuentre protegido y agrupado, separado de las instalaciones eléctricas y de cierta forma aislado de algunas de las fuentes EMI. El recorrido que siguen los medios de transmisión desde los distribuidores hasta los puntos terminales en los clientes, se garantiza y ordena mejor cuando es dentro de canaletas diseñadas para medios de transmisión de datos. Por lo general el tamaño de las canaletas dependerá del número de medios de transmisión que contenga.

2.2.2.5 Etiquetado y documentación

Es importante que toda infraestructura de transporte estructurada se complete con un etiquetado claro y duradero. La identificación de cables entre extremos luego del etiquetado debe ser fácil, y debe constar en un documento dotado de tablas y planos descriptivos de la instalación.

2.3 SISTEMA DE CABLEADO ESTRUCTURADO COMO INFRAESTRUCTURA DE TRANSPORTE DE UNA RED ESTRUCTURADA DE DATOS

Hasta el momento se ha tratado a la infraestructura de transporte de una manera relativamente general, tratando de hacer diferenciaciones entre una infraestructura de transporte tradicional y una infraestructura de transporte estructurada.

Debe notarse que si bien la infraestructura de transporte de datos tradicional presenta un costo inicial bajo con relación a una infraestructura de transporte estructurada, los cambios, reubicaciones, nuevas instalaciones, y en general solución de problemas, son atendidos con mucha mayor flexibilidad, eficiencia y bajo costo cuando se utiliza una infraestructura de transporte estructurada de datos.

Actualmente se cuenta con una solución de infraestructura de transporte que integra recursos tales como: telefonía, telefax, LANs, sistemas de audio y video, seguridad, etc. Los enlaces de transmisión están clasificados en cuatro áreas de aplicación. La característica que permite esta clasificación es principalmente el ancho de banda que dicha aplicación requiere. La tabla 2.14 resume esta clasificación.

Clase	Campos de aplicación
A	Protocolos de transmisión de bajas tasas de bits. Ej: señales de sistemas de control, señales de voz. En general, enlaces de transmisión especificados hasta 100 KHz.
B	Protocolos de transmisión de medianas tasas de bits. Ej: Conexión básica ISDN, señales de sistemas de control. En general, enlaces de transmisión especificados hasta 1 MHz.
C	Protocolos de transmisión de altas tasas de bits. Ej: Ethernet, *Token-Ring*. En general, enlaces de transmisión especificados hasta 16 MHz.
D	Protocolos de transmisión de muy altas tasas de bits. Ej: FDDI, ATM, 100BaseVG. En general, enlaces de transmisión especificados hasta 100 MHz.

***Tabla 2.14** Areas de aplicación de los enlaces de transmisión dependiendo de su clase*

Las longitudes de canal que se pueden alcanzar con las diferentes categorías y tipos de cableado se muestran en la tabla 2.15.

Un sistema de cableado estructurado debe permitir modificaciones y ampliaciones para soportar cualquier servicio de transmisión actual o futura, siendo lo suficientemente flexible para incorporar cualquier innovación tecnológica, sin requerir nuevos tendidos de cable, y garantizando funcionabilidad por un período comprendido entre 10 y 15 años.

Este criterio, es principalmente aplicable en instalaciones donde el número de usuarios y su densidad por planta son suficientemente elevados, permitiendo su fácil reubicación con bajo costo, y facilitando la administración y mantenimiento de la red.

Medio	Longitud del canal			
	Clase A	Clase B	Clase C	Clase D
Cable bal. Cat. 3	2 Km	200 m	100 m (1)	
Cable bal. Cat. 4	3 Km	260 m	150 m (2)	
Cable bal. Cat. 5	4 Km	260 m	160 m (2)	100 m (1)

(1) La distancia de 100 m incluye el total permitido de 10 m de cable flexible para *patch-cords*/-jumper, área de trabajo y conexiones de equipo

(2) Para distancias más grandes que 100 m de cable balanceado, en el subsistema de cableado horizontal, se deberían aplicar los estándares de aplicación correspondientes

***Tabla 2.15** Longitudes permitidas dependiendo de la categoría del cable y de la clase de aplicación que se requiera*

Para la implementación de un sistema de cableado estructurado, deben ser consideradas las normas *Commercial Building Wiring Telecommunication Standard* de *EIA/TIA 568 (Electronic/Telecommunications Industries Association).*

Además se debe cumplir con todas las normas de comunicación de redes: ISO/ OSI, ANSI, IEEE, FDDI, RDSI, etc).

2.3.1 NORMAS Y ESTÁNDARES (ANSI/EIA/TIA)

Dentro de los principales estándares orientados a un sistema de cableado estructurado están los siguientes:

- ANSI/EIA/TIA-568-A (Commercial Building Telecommunications Cabling Standard)
- ANSI/EIA/TIA-569 (Commercial Building Standard for Telecommunications *Pathways* and Spaces)
- ANSI/TIA/EIA-606 (Administrative Standard for the Telecommunications Infrastructure of Commercial Buildings)
- ANSI/EIA/TIA-607 (Commercial Building Grounding and Bonding Requirements for telecommunications)

2.3.1.1 ANSI/EIA/TIA-568-A (Commercial Building Telecommunications Cabling Standard)

Este estándar fue inicialmente desarrollado a comienzos del año 1985 como un estándar para sistemas de cableado de telecomunicaciones de edificios. Las revisiones de este estándar se realizan cada 5 años. Así, este estándar reemplaza al estándar ANSI/EIA/TIA-568 de Julio de 1991.

El propósito de este estándar es especificar un sistema genérico de cableado de telecomunicaciones para edificios comerciales que soportarán un ambiente multiproducto y multivendedor.

Debe recordarse que la instalación de los sistemas de cableado durante la construcción o renovación del edificio es significativamente menos costosa y destructiva que después de que el edificio esté ocupado.

El alcance del estándar tiende a especificar los requerimientos mínimos para cableado de telecomunicaciones dentro de un edificio comercial, hasta e incluyendo los conectores y salidas de telecomunicaciones, y entre edificios, en un ambiente de campus. Se hacen especificaciones de requerimientos, distancias de cableado, configuraciones de conectores y salidas de telecomunicaciones, y topología recomendada.

El estándar intenta soportar un amplio rango de diferentes edificios comerciales y aplicaciones (voz, datos, video, texto e imagen). Típicamente esto incluye sitios con una extensión geográfica de hasta 3000 m, con 1000000 m^2 de espacio de oficina, y con una población de hasta 50000 usuarios.

Este estándar establece una vida útil mínima de la infraestructura de cableado de 10 años.

El estándar, hace referencia a una serie de definiciones, acrónimos y abreviaturas, a los que se tiene acceso en el mencionado estándar.

En su desarrollo se hace referencia a las siguientes partes:

1. Cableado horizontal
2. Cableado de *Backbone* (vertical)
3. Area de trabajo
4. Armario o *closet* de telecomunicaciones
5. Cuartos de equipos
6. Facilidades de entrada

A. Cableado horizontal

De lo que ya se ha expuesto en la presente tesis, dentro del cableado horizontal, es importante que se consideren las siguientes recomendaciones hechas en el presente estándar:

- Se recomienda una topología en estrella
- Los empalmes y puentes no son permitidos como parte del sistema de cableado horizontal de cobre
- La máxima distancia horizontal será de 90 m, independiente del tipo de medio.

- Las limitaciones de longitud para cables de conexión e interconexión (*patch cords*) no deberían exceder los 6 m. En la estación de trabajo pueden utilizarse cables que unan la salida y la estación de hasta 10 m.
- Se hace el reconocimiento de 3 cables para uso en el sistema de cableado horizontal:
    a. UTP de 4 pares de 100 Ω
    b. STP-A de 2 pares de 150 Ω
    c. Cable de fibra óptica 62,5/125 µm, de 2 fibras
- Se recomienda un mínimo de 2 salidas de telecomunicaciones para cada área de trabajo individual: la una con cable UTP de 100 Ω categoría 3 o más, y la otra con cable UTP cat. 5, STP-A, o cable de 2 fibras 62,5/125 µm.

B. Cableado de *backbone*

Tiene como función principal la interconexión entre los armarios de telecomunicaciones, cuarto de equipos e infraestructura de entrada de un sistema de cableado estructurado.

Consiste de cables de *backbone*, conexiones de cruce intermedios y principales, terminaciones mecánicas, y *patch cords* usados para conexiones de cruce de *backbone* a *backbone*.

Dentro de las recomendaciones sugeridas están las siguientes:

- Se recomienda utilizar una topología en estrella jerárquica. Se deberá tener dos niveles jerárquicos como máximo de conexiones de cruce en cableado de *backbone*. Desde la conexión de cruce horizontal, solamente se podrá atravesar una conexión de cruce para alcanzar la conexión de cruce principal. De esta manera, las interconexiones entre cualesquiera 2 conexiones de cruce horizontal pasarán a través de 3 o menos conexiones de cruce.
- Los cables reconocidos para cableado de *backbone* son:
    a. Cable UTP de 100 Ω
    b. Cable STP-A de 150 Ω
    c. Cable de fibra óptica 62,5/125 µm
    d. Cable de fibra óptica monomodo

- Las distancias máximas son dependientes de la aplicación:
    a. Cable de *backbone* UTP cat. 3, para aplicaciones cuyo ancho de banda esté en el rango de los 5 a 16 MHz, debería estar limitado a una distancia de 90 m.
    b. Cable de *backbone* UTP cat. 4, para aplicaciones cuyo ancho de banda esté en el rango de los 10 a 20 MHz, debería estar limitado a una distancia de 90 m.

c. Cable de *backbone* UTP cat. 5, para aplicaciones cuyo ancho de banda esté en el rango de los 20 a 100 MHz, debería estar limitado a una distancia de 90 m.
d. Cable de *backbone* STP-A de 150 Ω, para aplicaciones cuyo ancho de banda esté en el rango de los 20 a 300 MHz, debería estar limitado a una distancia de 90 m.
e. En la figura 2.23, se muestran las máximas distancias permitidas de acuerdo al tipo de cable mostrado en la tabla 2.16.

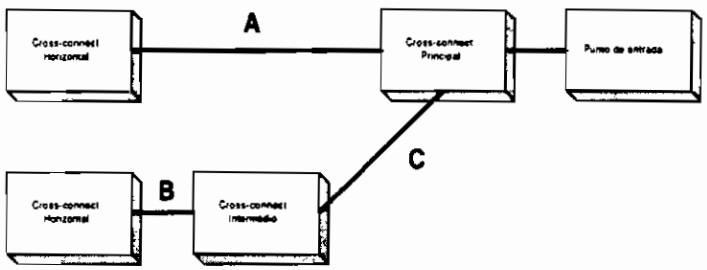


***Figura 2.23** Distancias entre elementos de cableado*

Tipo de medio	A	B	C
UTP	800 m	500 m	300 m
FO 62,5 µm	2000 m	500 m	1500 m
FO Monomodo	3000 m	500 m	2500 m

***Tabla 2.16** Distancias entre elementos de cableado*

La distancia desde el *Cross-conect* Horizontal al *Cross-connect* Principal no excederá el máximo de 2000 m para FO de 62,5 µm o 3000 m para FO de monomodo.
La distancia del *Cross-connect* Intermedio al *Cross-connect* Principal para cable UTP puede ser incrementada, pero el total de la distancia desde el *Cross-connect* Horizontal al *Cross-connect* Principal no excederá el máximo de 800 m.

- En el *Cross-connect* principal y en el *Cross-connect* Intermedio, las longitudes de los *patch cords* no excederán los 20 m.
- El equipo de telecomunicaciones que se conecta directamente a los *cross-connect* principal e intermedio, deberá hacerlo con cables (cables del equipo) de 30 m. o menos.

C. Area de trabajo

Deben considerarse las siguientes recomendaciones:

- La longitud máxima del *patch cord* será de 3 m en el área de trabajo.

- Cuando sean requeridos adaptadores específicos de la aplicación, ellos serán externos a la salida/conector (salida) de telecomunicaciones. Entre los más comunes se encuentran:
    a. Un cable especial o adaptador se requiere cuando el conector del equipo es diferente de la salida de telecomunicaciones
    b. Un adaptador "Y" es requerido cuando 2 servicios corren sobre el mismo cable
    c. Adaptadores pasivos pueden ser necesarios cuando el tipo de cableado horizontal es diferente del tipo de cable requerido por el equipo.
    d. Adaptadores activos pueden ser necesarios cuando se conectan dispositivos que utilizan esquemas de señalización diferente.
    e. En algunos casos, la transposición de pares puede ser necesaria por compatibilidad.
    f. Algunos equipos de telecomunicaciones requieren terminaciones de resistencia en el área de trabajo

D. *Closets* de telecomunicaciones

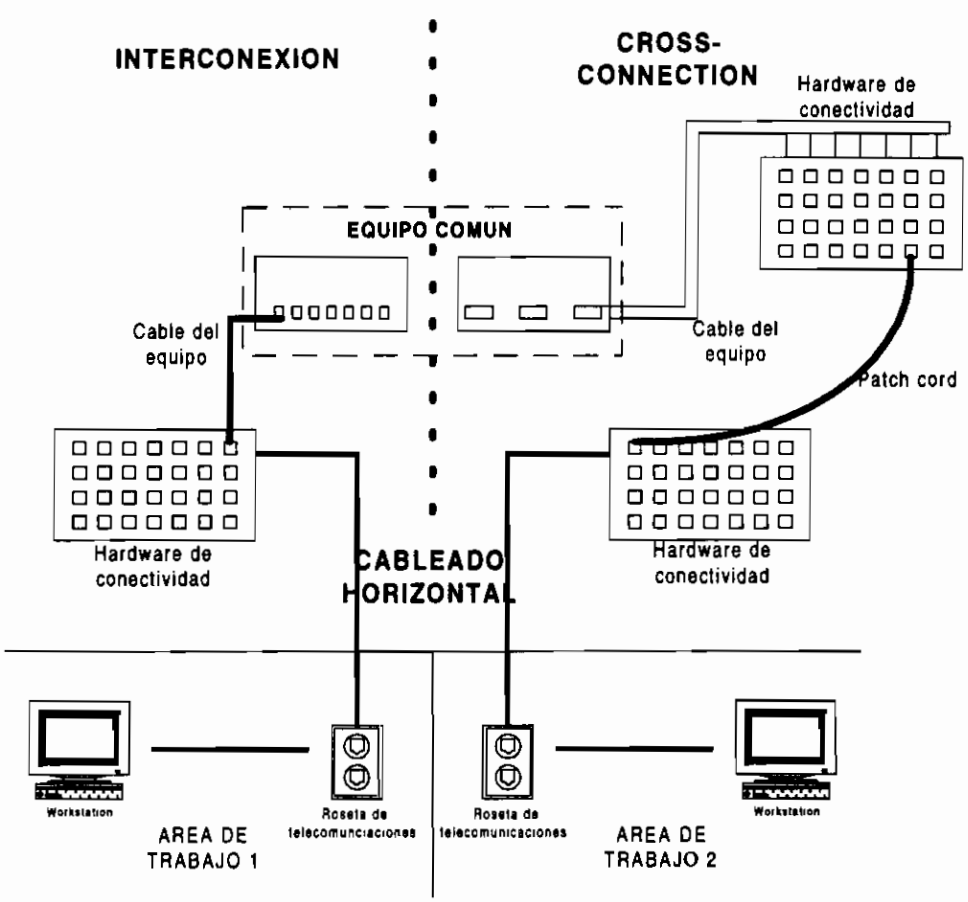


***Figura 2.24** Diferenciación entre interconexión y conexión de cruce*

La función primaria del *closet* de telecomunicaciones es proveer la terminación de la distribución del cableado horizontal. Similarmente, los tipos

de cable de *backbone* son también terminados en el *closet* de telecomunicaciones sobre el *hardware* de conectividad compatible. Se deben observar precauciones en el manejo del cable, incluyendo la eliminación de tensión excesiva del cable.

Sobre las conexiones de cruce e interconexiones, debe considerarse que los cables de tendido horizontal y *backbone* deberán ser terminados sobre *hardware* de conectividad que cumpla con los requerimientos del estándar. Estas terminaciones de cable no serán usadas para administrar el sistema de cableado. Todas las conexiones entre cables de tendido horizontal y *backbone* serán hechas a través de un *cross-connect* horizontal.

En la figura 2.24 se puede ver que el cableado horizontal en el área de trabajo 1 es interconectado al equipo común, mientras que el cableado horizontal en el área de trabajo 2 realiza una conexión de cruce al equipo común.

E. Cuarto de equipos

Los cuartos de equipos son considerados distintos de los *closets* de telecomunicaciones debido a la naturaleza o complejidad que ellos contienen. Los cuartos de equipo serán diseñados y provisionados de acuerdo a los requerimientos del estándar ANSI/EIA/TIA-569.

F. Facilidades de entrada

Consiste de los cables, *hardware* de conectividad, dispositivos de protección y otro equipo necesario para conectar la salida de la planta a las premisas de cableado. Estos componentes podrían ser usados para servicios de red pública, privada o ambos. El punto de demarcación entre los proveedores de servicio y el cliente podría ser parte de la facilidad de entrada.

Los *pathway* y spaces (canaletas y bandejas) serán designados e instalados de acuerdo a los requerimientos del ANSI/EIA/TIA-569.

2.3.1.2 ANSI/EIA/TIA-569 (Commercial Building Standard for Telecommunications *Pathways* and Spaces)

Este estándar hace referencia a la parte física (canaletas, tubería y bandejas) que servirá de soporte para el sistema de cableado que se monte sobre él. El estándar reconoce conceptos fundamentales relativos al dinamismo con la que varían las telecomunicaciones y edificios. Adicionalmente hace mención de que las telecomunicaciones no son solo voz y datos, sino además servicios tales como control ambiental, seguridad, audio, televisión, sensorización, alarmas y *paging*. De esta manera, hace referencia a las telecomunicaciones como la integración de sistemas de señales de bajo voltaje dentro de los edificios.

El propósito de este estándar es especificar prácticas de diseño y construcción dentro y entre edificios, los cuales sean el soporte de los medios y equipamiento de las telecomunicaciones.

Este estándar generalmente no hace recomendaciones sobre las alternativas de diseño disponibles. Por ejemplo, la elección entre un sistema conduit versus un sistema de bandeja.

El estándar no cubre aspectos de seguridad del diseño de edificios; para ello existen estándares determinados.

Entre los elementos de construcción básicos se encuentran:

1. Canaletas de tendido horizontal (*Horizontal Pathways*)
2. Canaletas de tendido de *backbone* (*Backbone Pathways*)
3. Estación de trabajo
4. *Closet* de telecomunicaciones
5. Cuarto de equipos
6. Facilidades de entrada:
    - 6.1 Cuarto de entrada o espacio
    - 6.2 Entrada de servicio
    - 6.3 *Backbone* entre edificios
    - 6.4 Entrada alterna
    - 6.5 Entrada de antena

El estándar, hace referencia a una serie de definiciones, acrónimos y abreviaturas, que han sido ya utilizados en la presente tesis, pero con terminología en español.

2.3.1.3 ANSI/TIA/EIA-606 (Administrative Standard for the Telecommunications Infrastructure of Commercial Buildings)

Este estándar será tratado en la parte correspondiente a "Administración de la infraestructura de transporte de una red estructurada de datos" en el numeral 2.5 de este mismo capítulo.

2.3.1.4 ANSI/EIA/TIA-607 (Commercial Building Grounding and Bonding Requirements for telecommunications)

El estándar 607 no está dentro del marco de estudio de la presente tesis, sin embargo es importante recordar que tiene aplicación dentro de todas las partes a implementar en cableado estructurado. Por tanto, para cualquier implementación práctica, deben seguirse las recomendaciones dadas en este estándar que fundamentalmente se refieren a la forma de realizar conexiones correctas a tierra.

2.3.2 SUBSISTEMAS DEL SISTEMA DE CABLEADO ESTRUCTURADO COMO INFRAESTRUCTURA DE TRANSPORTE

Un sistema de cableado estructurado es un ejemplo de un subsistema de infraestructura de transporte estructurado, el cual integra en general cualquier sistema informático o de comunicaciones. El sistema de cableado estructurado puede ser divido en los siguientes subsistemas:

a. Subsistema de campus
b. Subsistema vertical, troncal o *backbone* de edificio
c. Subsistema horizontal o de piso

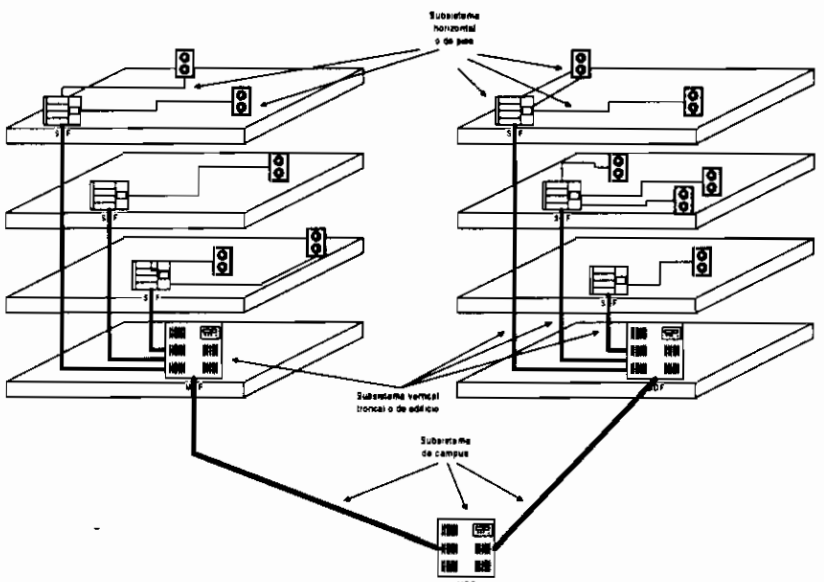


***Figura 2.25** Infraestructura de transporte estructurada y sus partes principales*

2.3.2.1 Subsistema de campus

El subsistema de campus está formado por las siguientes partes:

A. Distribuidor de campus

Sirve a un grupo de edificios. Utiliza *patch panels*, *patch/line cords*, productos para ambientes *host*/computador, y adaptadores/baluns.

B. Cableado de campus

Conecta entre edificios. Utiliza generalmente cables de fibra óptica.

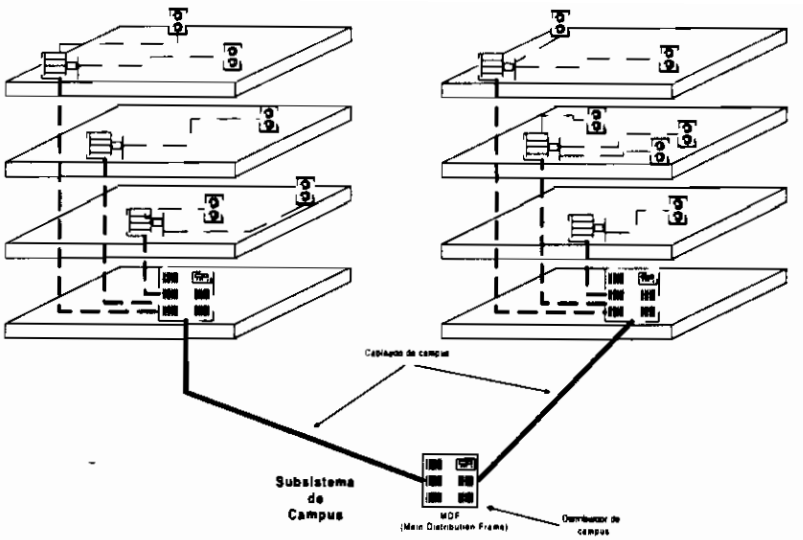


Figura 2.26 Subsistema de campus

El subsistema de campus, puede aceptar varias topologías, en anillo, en estrella, o en bus. Pueden ser incorporados sistemas de conexiones, voz y datos.

2.3.2.2 Subsistema vertical de edificio

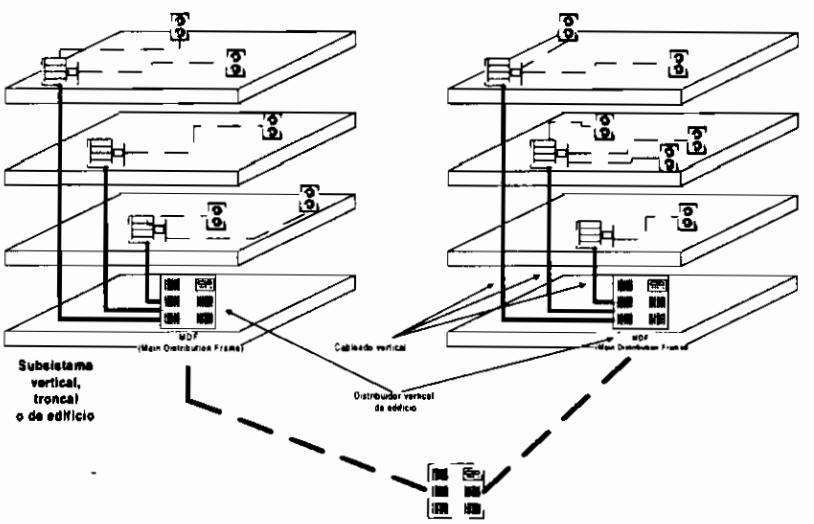


Figura 2.27 Subsistema vertical, troncal o de edificio (MDF)

El subsistema vertical de edificio está formado por las siguientes partes:

A. Distribuidor de edificio

Sirve un edificio entero. Utiliza *patch panels*, *patch/line cords*, productos para ambientes *host*/computador, y adaptadores/baluns.

B. Cableado vertical

Conecta entre pisos dentro de un edificio. Utiliza generalmente cables de fibra óptica y/o S-FTP, FTP o UTP.

Las aplicaciones que pueden aceptar son LAN en banda base, LAN en banda ancha y canales multiplexados.

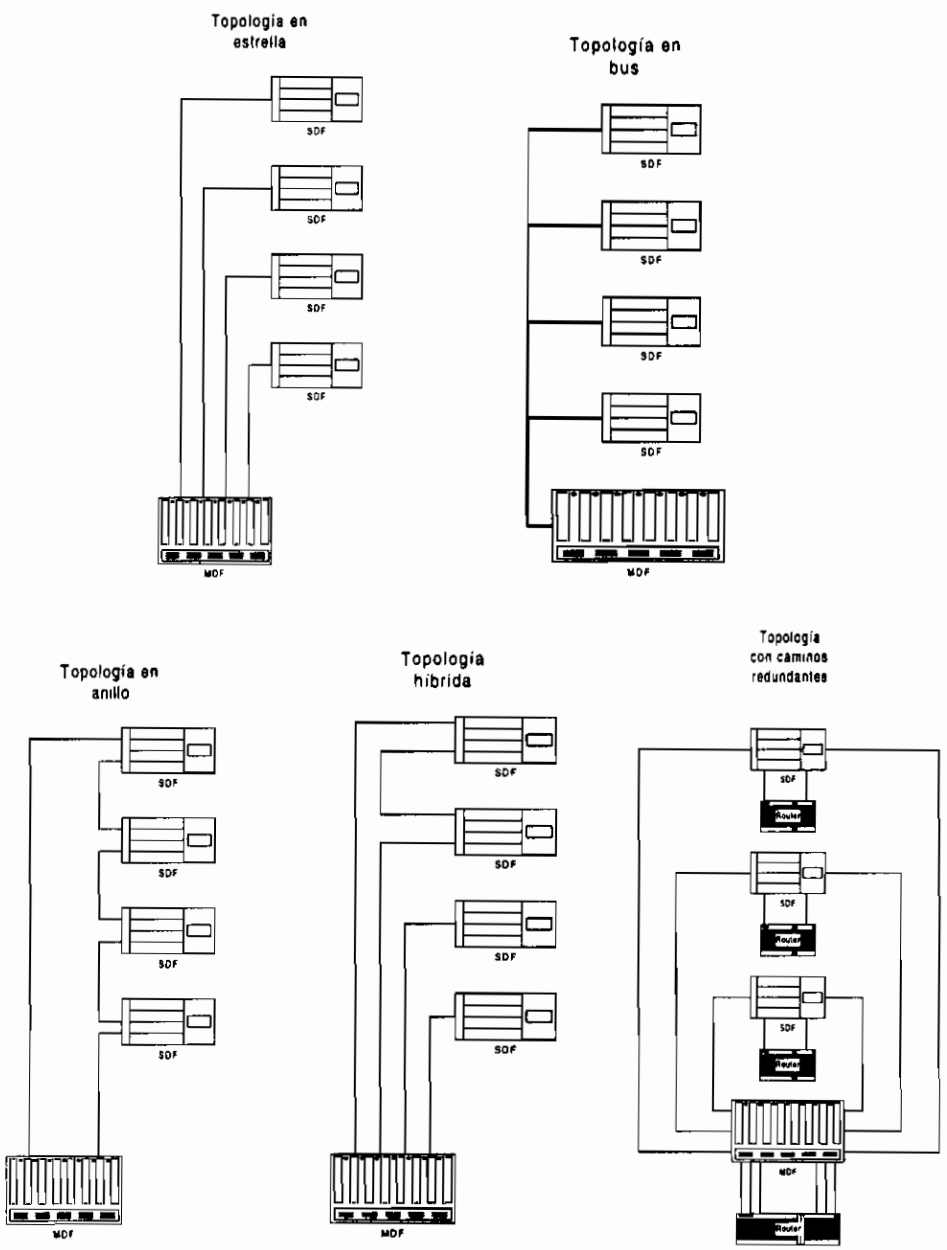


***Figura 2.28* Topologías utilizables para configuración del backbone**

La configuración del *backbone* puede utilizar varias topologías (ver figura 2.28), dependiendo de la necesidad que se presente:

a. *Backbone* en estrella
b. *Backbone* óptica en bus
c. *Backbone* en anillo
d. *Backbone* con topología híbrida
e. *Backbone* con caminos redundantes

2.3.2.3 Subsistema horizontal o de piso

El subsistema horizontal o de piso está formado por las siguientes partes:

A. Distribuidor de piso

Sirve un único piso de un edificio. Utiliza paneles terminales (*patch panels*), *patch/line cords*, productos para ambientes *host*/computador, y adaptadores/baluns.

B. Cableado horizontal

Conecta desde el distribuidor de piso al lugar de trabajo del usuario. Utiliza cables de fibra óptica y/o S-FTP, FTP o UTP y a esta parte de cable se la conoce como cable de tendido (*drop cable*). Incluye también cajas de conexión (*wall jack*) y los cables terminales (*patchcords*).

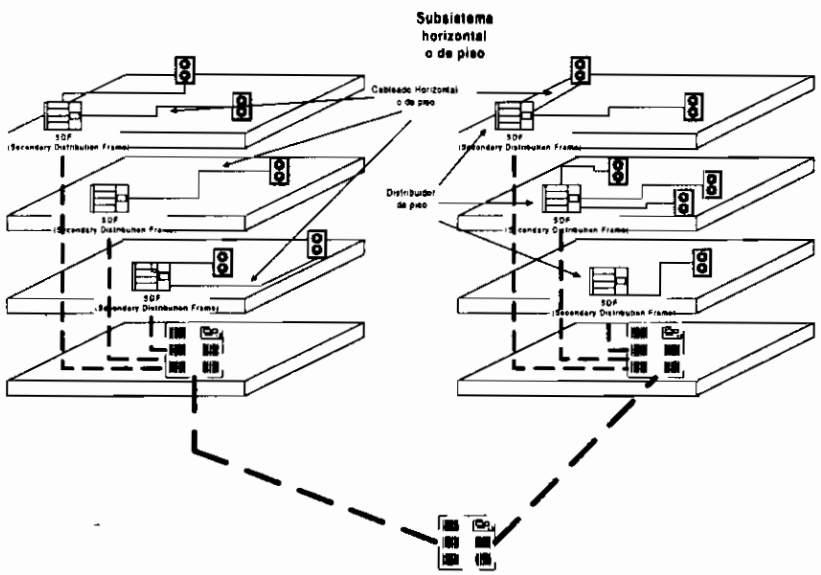


Figura 2.29 Subsistema horizontal o de piso (SDF)

El cableado horizontal generalmente representa sobre el 90% del cable en la instalación, lo que es una proporción significativa del costo. Además, el cableado horizontal estará oculto en el piso, techo y paredes, por lo que cualquier reubicación en el futuro puede resultar cara y dificultosa. Esto

significa que el segmento horizontal del cableado debe ser bien planificado y diseñado.

2.3.3 DESCRIPCIÓN DE LOS ELEMENTOS DE LOS SUBSISTEMAS DEL SISTEMA DE CABLEADO ESTRUCTURADO

En la sección 2.1.1 "Partes de la infraestructura de transporte" de este mismo capítulo, se trataron varias partes que están incluidas dentro del sistema de cableado estructurado. Sin embargo, se debe recordar que en la sección mencionada se hace referencia a una infraestructura de transporte estructurada pero de manera general, es decir no se hacen consideraciones en cuanto a las normas que actualmente son las que rigen el comportamiento de un sistema de cableado estructurado, sino que más bien fueron las bases sobre las que crecieron las normas que simplifican el sistema de cableado diversificado hacia un sistema de cableado homogéneo.

Esto no significa que únicamente el cableado estructurado es una infraestructura de transporte estructurada, sino que es la que actualmente se encuentra normalizada y ahí está su ventaja. Es importante esta aclaración, pues se podía haber hablado de una infraestructura de transporte estructurada, incluso antes de que despegara el concepto de cableado estructurado, siempre y cuando la infraestructura de transporte a la que se haga referencia, cumpla con los requerimientos de un sistema estructurado. De aquí, que proyectándonos hacia un futuro tal vez no muy lejano, el sistema de cableado estructurado pase a ser una infraestructura de transporte estructurada pero obsoleta, pues quizás las normas dirán que el sistema que regirá utilizará infraestructuras de transporte de datos sin cable, sin embargo la filosofía que hará de un sistema cualquiera un sistema estructurado, seguirá manteniéndose.

Los elementos comunes a los subsistemas de cableado estructurado son los siguientes:

1. Cajas de conexión
2. Cables y conectores
3. Adaptadores, baluns, empalmes y uniones
4. Canaletas
5. Paneles de distribución
6. Bloques de conexión con módulos IDC
7. Gabinetes o *racks*
8. Etiquetado
9. Pruebas y documentación

2.3.3.1 Cajas de conexión o salidas de telecomunicaciones

Las cajas de conexión o salidas son los dispositivos que van instaladas en el lugar de trabajo de usuario. Está formada principalmente por tres partes:

- Caja
- Módulo de conexión
- Placa frontal

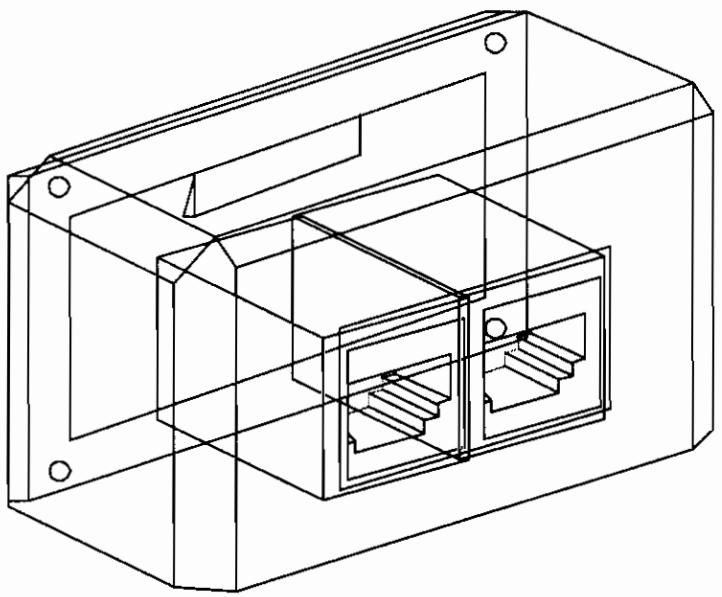


Figura 2.30 Caja de conexión o salida

A. Para cable UTP

La caja se coloca contra la superficie de instalación y es la base posterior de la salida. En algunos casos posee caminos construidos que sirven para organizar el cable que irá conectado al módulo de conexión.

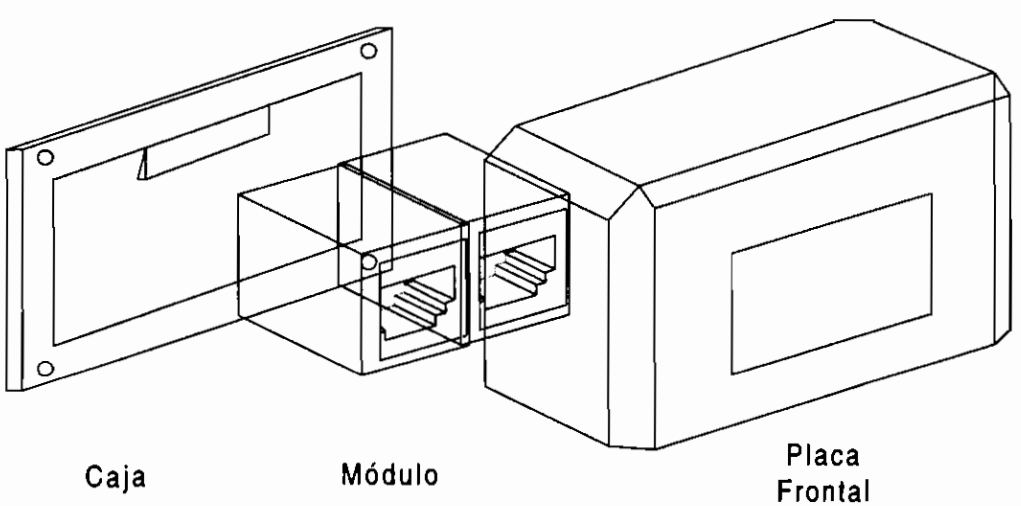


Figura 2.31 Partes principales de una caja de conexión o salida

La mayoría de fabricantes presentan un módulo de conexión que en su parte frontal utiliza un conector RJ45 hembra, y en su parte posterior utiliza un

conector IDC (*Insulation Displacement Contact*) Algunos fabricantes, como IBM por ejemplo, poseen módulos de conexión que utilizan una técnica de terminación que llaman "*Easy Lock*", mediante la cual se permite conectar el cable a la parte trasera del módulo, sin requerir herramienta, ya que el mismo módulo posee un seguro que permite apretar el cable fácilmente.

De esta manera, el cableado horizontal procedente del distribuidor de planta o piso, llegará dentro de la caja y se conectará al dispositivo de conexión por desplazamiento de aislamiento (IDC). En la parte frontal quedará disponible el conector hembra RJ45 para que ahí se conecte el cable terminal (*patch cord*) de usuario que irá al teléfono o a su equipo de datos. En algunos casos, el módulo de conexión posee una angulación (de aproximadamente 30°) en la parte frontal (donde está el conector RJ45 hembra), con el fin de proteger los contactos de la acumulación de polvo.

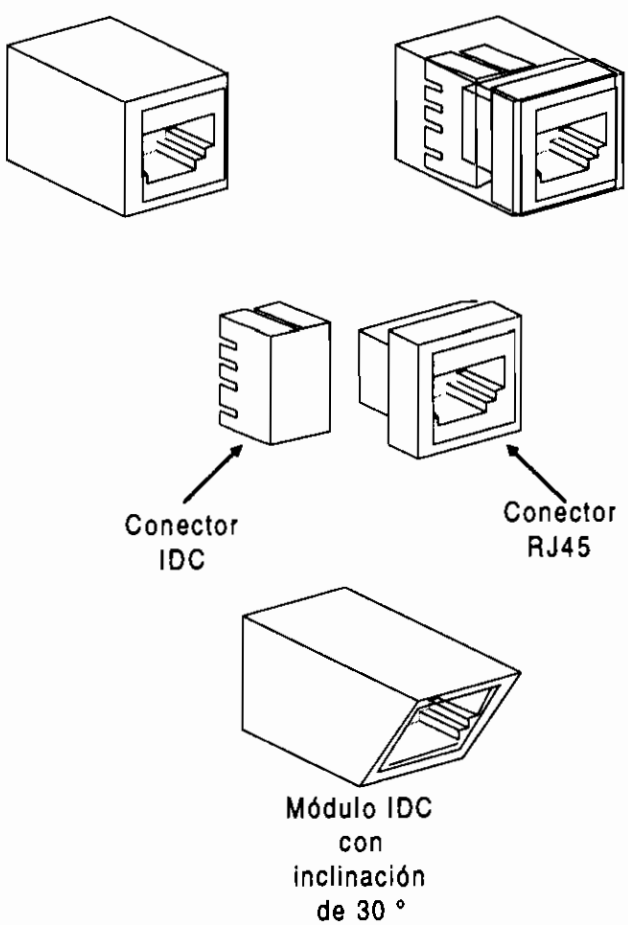


***Figura 2.32* Módulos de conexión**

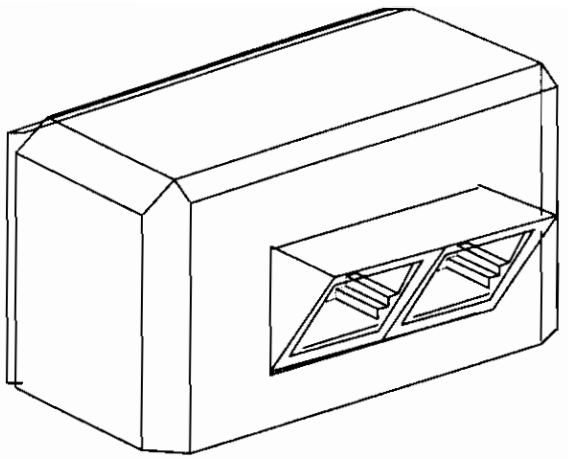


Figura 2.33 Caja de conexión armada de módulos con inclinación

El módulo de conexión presenta la siguiente distribución para una conexión de datos cuando utiliza polaridad WE8W (ó RJ45) y secuencia EIA 568B[17]:

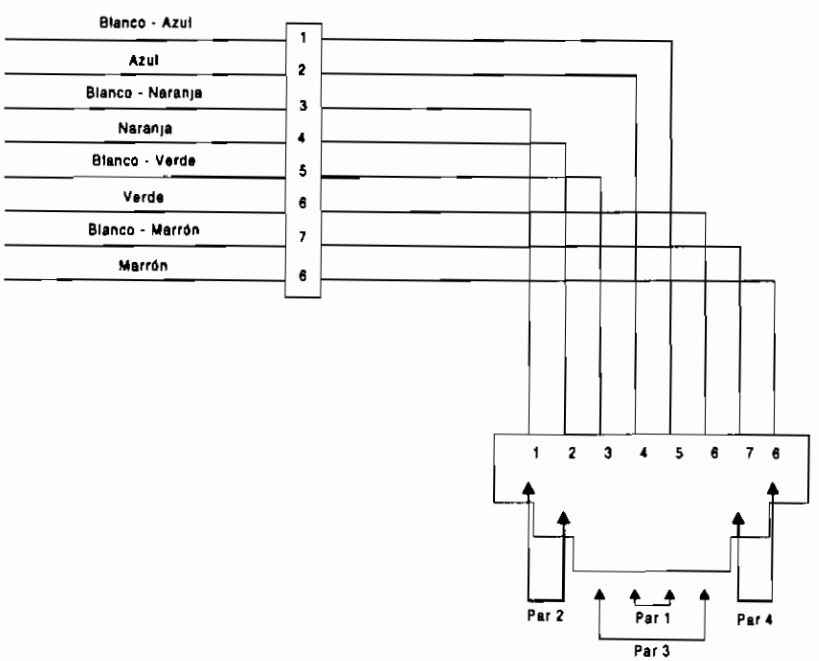


Figura 2.34 Distribución de cables utilizando secuencia EIA 568B

La placa frontal está diseñada para cubrir y sostener los módulos de conexión con la caja, completando de está forma una estructura compacta. Por lo general, las placas frontales permiten que los módulos de conexión sean dispuestos en

[17] Ver lo correspondiente a polaridad y secuencia en el Anexo - Polaridad y Secuencia -

grupos de dos. Otra de las funciones de la placa frontal, es permitir un correcto etiquetado del servicio disponible en el conector.

La mayoría de fabricantes de cajas de conexión buscan fundamentalmente lo siguiente:

- Cumplir especificaciones categoría 5 (la buena conductividad de los conectores se consigue revistiendo oro sobre la superficie generalmente de níquel de los contactos)
- Estabilidad dimensional
- Reducción del desgaste provocado por uso continuado
- Eliminación de fallos debidos a vibraciones de contactos
- Confiabilidad en transmisiones de alta velocidad
- Resistencia térmica
- Facilitar el etiquetado, de tal forma que sea difícil equivocarse en la elección del servicio y por otro lado que se facilite la documentación.

B. Para cable de fibra óptica

En lo referente a caja y placa frontal, las características son análogas a las de cable UTP, sin embargo, existen diferencias en los módulos de conexión. Los tipos de conectores de fibra óptica que se soportan generalmente son: ST, SC.

2.3.3.2 Cables y conectores

A. Cable de par trenzado

. El cable de par trenzado se lo puede encontrar en varias categorías (3, 4, 5) y clases (UTP, STP, FTP, S-FTP) como se mostró anteriormente en este mismo capítulo, en la parte correspondiente a medios de transmisión.

Los más ampliamente utilizados en cableado estructurado por sus características de costo, maniobrabilidad y por ser aptos para soportar aplicaciones que van desde bajos hasta los más altos requerimientos actuales son los cables UTP y FTP categoría 5.

En general los cables UTP, FTP y S-FTP categoría 5, soportan aplicaciones que van hasta los 100 MHz, para distancias menores a los 100 m. Estas aplicaciones podrían ser las siguientes: ATM, CDDI (FDDI sobre cable de cobre), *Token-Ring* 4/16, Ethernet, AS400, 3270, RDSI, teléfono y otras.

Existen versiones de cable UTP y FTP que se construyen para no producir humo en caso de incendio, y además están libres de halógenos. Estas versiones de cable se las conoce como cables LSFR0H (*Low Smoke - Fire Retardant - Zero Halogen*).

Para reducir el tiempo de instalación, se utiliza también el código de colores de los pares para las bandas de conexión IDC de las salidas de la pared y los paneles de interconexión. La puesta a tierra de la pantalla (en el caso de FTP y S-FTP) se facilita conectando el hilo de drenaje de la pantalla a un terminal IDC de la salida y el panel de interconexión.

El tamaño de los cables UTP, FTP y S-FTP es conveniente que sea pequeño en diámetro, con el fin de facilitar las tareas de instalación y extracción. Es importante que estos cables mantengan determinado grado de rigidez con el fin de evitar los doblamientos extremos de 90° (típicos en cables pequeños en diámetro) que podrían ocasionar la degradación del cable y la perforación de las cubiertas.

Es importante que todos los tipos de cable mantengan una superficie exterior uniforme y con un bajo coeficiente de fricción con el fin de facilitar su instalación y extracción.

Estos cables, generalmente son fabricados en dos tipos:

- Cables para interiores de 4 pares
- Cables para cableado vertical e interiores de 25/50/100/150 y 200 pares aproximadamente

Algunas de las características más relevantes de los cables que se han mencionado se detallan en la tabla 2.17.

El conector más ampliamente utilizado para este tipo de cable es el conector WE8W ó RJ45 cuando se utiliza como cable terminal (desde equipo terminal de datos hasta salida). Para el cable de tendido horizontal (es decir desde la salida hasta el distribuidor de planta o piso) el tipo de conexión que generalmente se utiliza es IDC en los dos extremos. Los cables terminales que conectan el panel de distribución horizontal con el "equipo activo" perteneciente al subsistema de conectividad, por flexibilidad a cambios y reasignaciones, generalmente utilizan conectores RJ45 en sus dos extremos, aunque esto depende del panel de distribución horizontal, ya que en muchos casos con el fin de reducir costos, se utilizan paneles con conectorización tipo IDC.

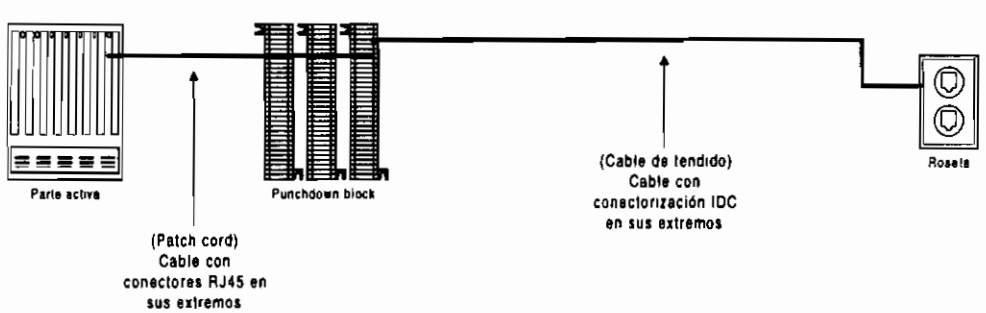


Figura 2.35 Configuración de conectorización utilizando regletas de bloque tipo 110

Cable→ ↓Especificaciones		UTP		FTP		S-FTP	
		4 pares	25/50../200 pares	4 pares	25/50../200 pares	4 pares	25/50../200 pares
Mecánicas							
Conductor		Cobre	Cobre	Cobre	Cobre	Cobre	Cobre
Calibre		0,5 mm 24 AWG	0,5 mm 24 AWG	0,5 mm 24 AWG	0,5 mm 24 AWG	0,5 mm 24 AWG	0,5 mm 24 AWG
Aislamiento		Polietileno	Polietileno	Polietileno	Polietileno	Polietileno	Polietileno
Apantallamiento 1		Ninguno	Ninguno	Aluminio	Aluminio	Aluminio	Aluminio
Apantallamiento 2		Ninguno	Ninguno	Ninguno	Ninguno	Cobre, tin-plated	Cobre, tin-plated
Cubierta		PVC	PVC	PVC	PVC	PVC	PVC
Rango de temperatura		-20° C a +70° C	-20° C a +70° C	-20° C a +70° C	-20° C a +70° C	-20° C a +70° C	-20° C a +70° C
Eléctricas y de transmisión							
Resistencia		≤ 75Ω/Km (c.c.)	≤ 85Ω/Km (c.c.)	≤ 75Ω/Km (c.c.)	≤ 85Ω/Km (c.c.)	≤ 75Ω/Km (c.c.)	≤ 85Ω/Km (c.c.)
Capacitancia		≤ 45nF/Km	≤ 45nF/Km	≤ 45nF/Km	≤ 45nF/Km	≤ 45nF/Km	≤ 45nF/Km
Impedancia Característica de 1-100 MHz		105 Ω ±10%	100 Ω ±10%	120 Ω ±10%	120 Ω ±10%	120 Ω ±10%	120 Ω ±10%
Ancho de Banda		100 MHz	100 MHz	100 MHz	100 MHz	100 MHz	100 MHz
Atenuación máx. (dB) /100m	Frecuencia	(Aprox.)	(Aprox.)	(Aprox.)	(Aprox.)	(Aprox.)	(Aprox.)
	1 MHz	2 dB	2 dB	2 dB	2 dB	2 dB	2 dB
	4 MHz	4 dB	4 dB	3 dB	4 dB	3 dB	4 dB
	10 MHz	6 dB	6 dB	5 dB	5 dB	5 dB	5 dB
	16 MHz	8 dB	8 dB	6 dB	6 dB	6 dB	6 dB
	25 MHz	10 dB	10 dB	7 dB	8 dB	7 dB	8 dB
	60 MHz	16 dB	17 dB	12 dB	13 dB	12 dB	13 dB
	100 MHz	22 dB	23 dB	16 dB	18 dB	16 dB	18 dB
Paradiafonía (NEXT)	Frecuencia	(Aprox.)	(Aprox.)	(Aprox.)	(Aprox.)	(Aprox.)	(Aprox.)
	1-25 MHz	- 44 dB	- 42 dB	- 50 dB	- 42 dB	- 50 dB	- 42 dB
	60 MHz	- 36 dB	- 35 dB	- 41 dB	- 37 dB	- 41 dB	- 37 dB
	100 MHz	- 32 dB	- 32 dB	- 35 dB	- 32 dB	- 35 dB	- 32 dB

Tabla 2.17 Especificaciones de cable de par trenzado

B. Cable de fibra óptica

Los cables de fibra óptica, dependiendo de la aplicación son factibles encontrarlos en las siguientes presentaciones:

- Cable de fibra óptica para interiores de 2 fibras preconectorizado
- Cable de fibra óptica para interiores de 2 fibras (sin conectorizar)
- Cable de fibra óptica para interiores "multipar" preconectorizado
- Cable de fibra óptica para cableado vertical "multipar" (sin conectorizar)

Normalmente se utiliza el cable de fibra óptica "multimodo" (no monomodo). Para interiores generalmente se utiliza cable de fibras ajustadas (conocida

también como configuración apretada), mientras que para vertical y exteriores se utiliza el cable de fibras libres (conocida también como configuración suelta).

El cable preconectorizado es recomendable en condiciones donde la instalación del cable de fibra óptica con sus conectores no entorpece la instalación, sino que la agilita. El grado de calidad del cable preconectorizado como producto final es mejor que el cable sin conectorizar una vez que el instalador pone los conectores. El cable sin conectorizar es recomendable en condiciones donde no se tiene certeza de parámetros como distancia y facilidad de instalación del cable.

Es por esta razón que el cable preconectorizado se utiliza principalmente en instalación de interiores en cableado horizontal, mientras que para el cableado vertical y de campus es más utilizado el cable sin conectorizar. Sin embargo, esta no es una norma rígida, sino como se mencionó en el párrafo anterior, dependerá de la condición del ambiente y del buen criterio del instalador.

La construcción compacta del cable de fibra óptica y su revestimiento, deben garantizar una buena protección mecánica, dándole al cable alta resistencia, buena flexibilidad y buena curvatura. Las fibras además vienen con codificación de colores, lo que facilita su identificación.

Los cables multipares son utilizados comúnmente en interiores (vertical) y exteriores (campus). Debido a que la estructura de estos cables está desprovista de metal, son muy robustos y adecuados para utilizarse donde se aplica tracción mecánica después del reposo, como en bandejas de muchos cables por ejemplo. Estos cables generalmente utilizan una cubierta exterior de polietileno negro para soportar condiciones de alta humedad, resistencia a cortes, corrosión y envejecimiento por rayos ultravioletas. Además algunos proveedores (como Alcatel por ejemplo), utilizan elementos de refuerzo de polímero de fibra reforzada para alcanzar gran estabilidad mecánica y protección contra los roedores. Este tipo de cables robustos pueden instalarse en bandejas, conductos o podrían ser enterrados directamente.

Al igual que en el cable de par trenzado, existen versiones de cable de fibra óptica que previene la contaminación y envenenamiento en caso de incendio, lo que se consigue utilizando materiales que estén libres de halógenos y humo.

Es importante que la cubierta exterior del cable conserve características de uniformidad y bajo coeficiente de rozamiento para simplificar las tareas de instalación y extracción del cable.

Algunas de las características más relevantes de los cables que se han mencionado se detallan en la tabla 2.18.

Tipo → ↓ Especificaciones	Cable de 2 fibras *	Cable multipar *
Mecánicas		
Tipo de fibra	62,5/125 µm	62,5/125 µm
Diámetro de recubrimiento	900 µm → fibras ajustadas	900 µm → fibras ajustadas 250 µm → fibras libres
Diámetro del tubo interior	3 mm	
Diámetro del cable	3,8 x 6,8 mm	7,5 mm → 8, 12, 36 fibras ajustadas 9,0 mm → 8, 12 fibras libres 12,2 mm → 36, 60 fibras libres
Cubierta exterior		Polietileno negro
Peso aprox.	32 Kg/Km → fibras ajustadas	25-50 Kg/Km → fibras ajustadas 7-12 Kg/Km → fibras libres
Fuerza de extracción máx.	1500 N → fibras ajustadas (en la instalación)	500 N → fibras ajustadas 1200 - 1700 N → fibras libres
Radio de curvatura mín.	35 mm	30 mm → fibras ajustadas 225-300 mm → fibras libres
Rango de temperatura	-10 a +60 °C	-10 a +60 °C → fibras ajustadas -30 a +60 °C → fibras libres
Opticas		
Atenuación máx.	850 nm 3,2 dB/Km 1300 nm 0,9 dB/Km	850 nm 3,2 dB/Km 1300 nm 0,9 dB/Km
Ancho de banda mín.	850 nm 200 MHz/Km 1300 nm 500 MHz/Km	850 nm 200 MHz/Km 1300 nm 500 MHz/Km

***Tabla 2.18** Especificaciones de cable de fibra óptica*

La mayoría de fabricantes y proveedores de cable de fibra óptica recomiendan utilizar el cable preconectorizado con el fin de mejorar la calidad y reducir el tiempo y costo de instalación. Sin embargo, como se mencionó en párrafos

* Cable sin conectores

anteriores, la situación práctica puede requerir que el montaje de los conectores sea obligatorio en la propia instalación.

2.3.3.3 Adaptadores, baluns, y empalmes o uniones (Interfaces)

Los adaptadores proveen una forma simple y compacta de cambiar secuencia y/o polarización. Se utilizan simplemente para convertir de un estilo de conector a otro, cuando el equipo a conectar tiene puertos de señales equilibradas pero que utilizan conectores distintos.

Normalmente se encuentran los siguientes tipos de adaptadores:

- Conector de datos IBM - RJ45 (patillas activas 4,5 y 3,6)
- RJ11 hembra - RJ45 hembra (teléfono, patillas activas 4,5)
- DB9 macho - RJ45 hembra (V24 - RS232)*
- DB25 macho - RJ45 hembra (V24 - RS232)*
- DB15 macho - RJ45 hembra (*)
- DB9 hembra - RJ45 hembra (V24 - RS232)*
- DB25 hembra - RJ45 hembra (802.5, patillas activas 3,6 y 4,5)*
- DB9 macho - RJ45 hembra (patillas activas 3,6 y 4,5)

Los baluns convierten señales balanceadas a no balanceadas y viceversa, adoptan las impedancias y convierten un tipo de conector a otro. Se utilizan cuando se requiere conectar un equipo con puertos de señales desequilibradas (o no balanceadas) a cable de par trenzado cuyas señales son equilibradas (o balanceadas).

Normalmente se encuentran los siguientes tipos de baluns:

- BNC macho - RJ45 hembra, 50-120 Ω (10Base2, patillas activas 4 y 5)
- BNC hembra - RJ45 hembra, 50-120 Ω (10Base2, patillas activas 4 y 5)
- BNC macho - RJ45 hembra, 75-120 Ω (CATV, Arcnet, patillas activas 4 y 5)
- BNC hembra - RJ45 hembra, 75-120 Ω (CATV, Arcnet, patillas activas 4 y 5)
- BNC macho - RJ45 hembra, 93-120 Ω (Arcnet, 3270, patillas activas 4 y 5)
- BNC hembra - RJ45 hembra, 93-120 Ω (Arcnet, 3270, patillas activas 4 y 5)
- Biaxial macho -RJ45 hembra, 105-120 Ω (biaxial, patillas activas 4 y 5)
- TNC/BNC macho -RJ45 hembra, 75-120 Ω (Wang coaxial, patillas activas 4,5 y 3,6)

En la figura 2.36 se muestran algunos tipos de baluns.

* Puede ser configurada por el usuario según la aplicación

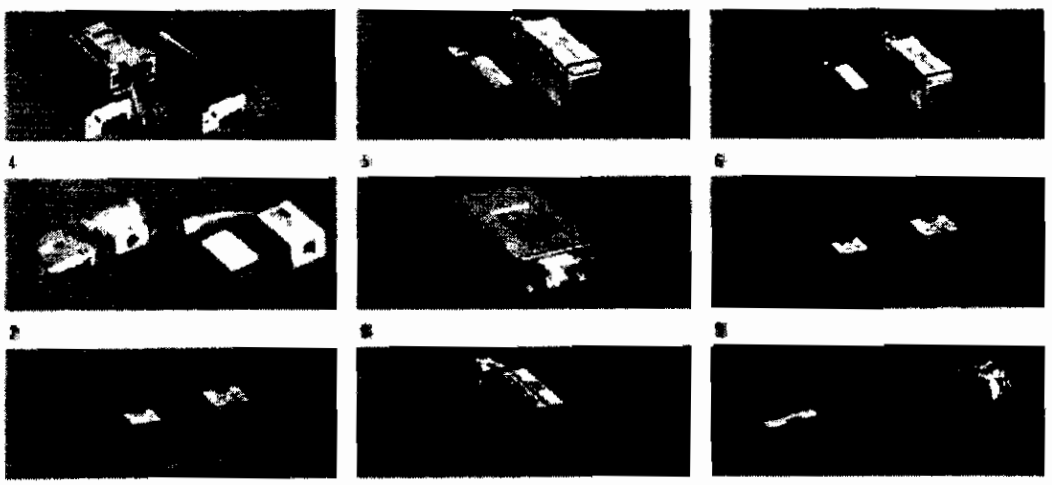


Figura 2.36 Ejemplos de balun

En la figura 2.37, se muestra un ejemplo de la configuración interna de un balun.

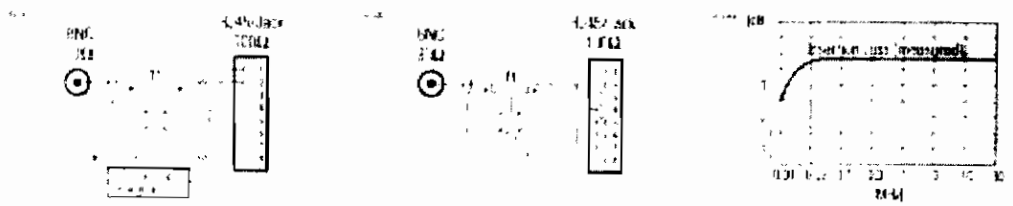


Figura 2.37 Ejemplo de configuración interna de un balun

En la figura 2.38 se muestra la conexión de un balun al *patch panel* y otro al lado de la salida.

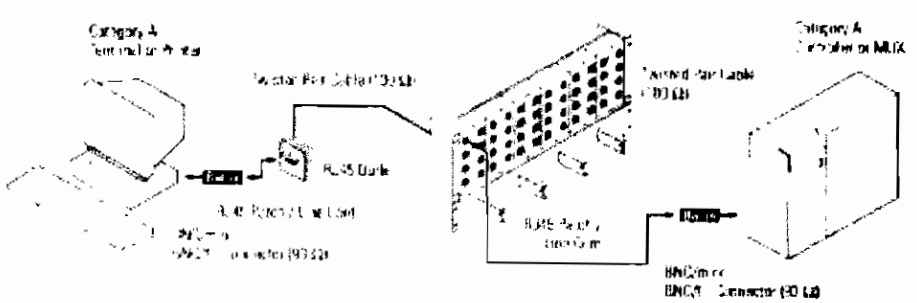
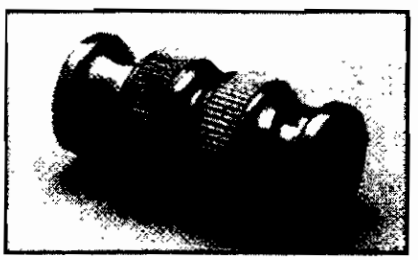


Figura 2.38 Utilización de baluns en la conexión de dispositivos

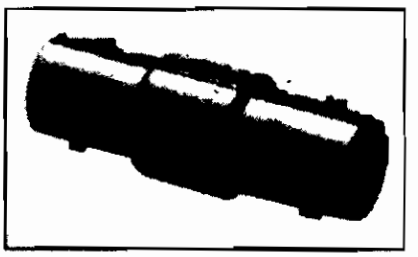
Los empalmes son técnicas que permiten conectar o "unir" dos cables de las mismas características, manteniendo sus especificaciones mecánicas, de

transmisión u ópticas en el caso de fibra óptica, generalmente con el objetivo de conseguir más distancia o terminar con conectores.

En la figura 2.39 se muestran dos uniones (macho y hembra) para conectores BNC.



BNC macho a BNC macho
27-8130P (empaque)



Empalme de linea BNC
25-7430P (empaque)

Figura 2.39 Unión para conectores BNC

Los empalmes no deben utilizarse en cables de par trenzado pues degradan su calidad. Para los cables de fibra óptica se utilizan principalmente 2 tipos de empalmes: de fusión y mecánicos. Si bien el empalme por fusión ofrece mejores características de pérdida de retorno y atenuación, el empalme mecánico avanzado le sigue de cerca debido a las altas tolerancias mecánicas de las fibras actuales y la utilización de componentes de ajuste del índice de refracción altamente controlado en la unión de fibras. Los empalmes mecánicos son también recomendables como piezas de repuesto emergentes.

2.3.3.4 Canaletas

Es importante que el cable se encuentre protegido y agrupado, separado de las instalaciones eléctricas y de cierta forma aislado de algunas de las fuentes EMI. El recorrido que siguen los medios de transmisión desde los distribuidores hasta los puntos terminales en los clientes, se garantiza y ordena mejor cuando está dentro de canaletas diseñadas para medios de transmisión de datos.

El tipo de canalización a utilizarse dependerá mucho del tipo de instalación que se esté realizando y de si existe canalización o debe instalársela. Generalmente el tipo de canalización que se utiliza para los sistemas de distribución de cableado de par trenzado es de PVC rígido autoextinguible, o de escalerilla de chapa perforada con tapa si es necesario, sometida a tratamientos superficiales anticorrosión. En el caso de la fibra óptica, se utilizan generalmente tubos de PVC autoextinguible y aislante con buena resistencia al impacto.

Desde las canaletas hasta las cajas de conexión de usuarios se utiliza generalmente tubo corrugado estanco de PVC autoextinguible reforzado

interiormente con espiral de PVC rígido o tipo TM-PVC (interior con fleje de acero galvanizado).

Para el caso de canaletas a la vista suele utilizarse canaletas de PVC con tapa.

Para sujetar los cables a las escalerillas, se utilizan correas y abrazaderas de sujeción autoblocantes, construidas de nylon no reactivo autoextinguible, resistentes a la grasa y agentes alcalinos.

Por lo general el tamaño de las canaletas dependerá del número de medios de transmisión que contenga.

2.3.3.5 Paneles de distribución

Los paneles de distribución (*patch panels*) son usados para terminar la instalación de cableado horizontal y vertical, y formar una interfaz a varios equipos de conectividad.

En el cableado horizontal, los puertos del panel de distribución son conectados en una topología física estrella por cables a las salidas de usuario. De esta forma, el equipo perteneciente al subsistema de conectividad (*hubs, switches, bridges, routers*) y si es el caso los equipos de telefonía (PABX), seguridad y control, podrán ser fácilmente conectados al panel de distribución mediante cables terminales (*patch cords*). Esto permite fácilmente asignar cualquier servicio a cualquier salida de usuario, permitiendo una administración centralizada y eficiente.

Para el cableado vertical y de campus, la estrategia es la misma que la utilizada para cableado horizontal, sólo que los distribuidores agruparán cables que ya no están conectadas a salidas de usuario, sino a otros distribuidores de planta o a otros distribuidores de edificio. Por la modularidad que tienen los paneles de distribución, puede utilizarse el mismo módulo para distribución de cableado horizontal, vertical y de campus.

Es importante mantener el orden de los cables terminales (*patch cords*) en los paneles de distribución para que la administración se facilite, además de guardar un correcto margen estético. Para este efecto, los fabricantes dotan a los paneles de distribución de guías de cableado y bandejas que permiten agrupar y ordenar con mayor facilidad el cableado, y además dotan los paneles de distribución de facilidades para el marcado y etiquetado.

Por norma, los paneles de distribución vienen en tamaños que les permite ser montados en gabinetes (*racks*) de 19' (482 mm). Además, la mayoría de fabricantes crean sus paneles de distribución con capacidad para 12, 16, 24, 48 y 96 puertos, teniendo un diseño modular, lo que permite que el instalador, agrupe paneles de distribución con el número de puertos que requiera, y de esa forma

será él quien configure su necesidad. La característica de modularidad además permite que en el futuro[18] puedan aumentarse más módulos para satisfacer las necesidades que se presenten.

Principalmente se fabrican 2 tipos de paneles de distribución:

a. Para cable de par trenzado (UTP, STP, FTP, -S-FTP)
b. Para fibra óptica

A. Paneles de distribución para par trenzado

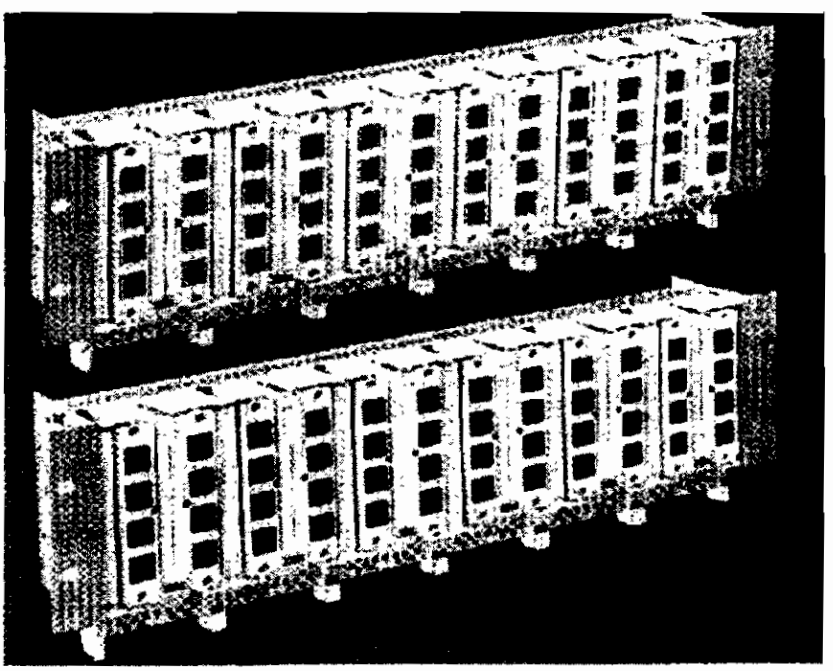


Figura 2.40 Patch Panel para conectores RJ45

Los paneles de distribución para cable de par trenzado en cableado estructurado poseen módulos con conectorización IDC en la parte posterior y RJ45 hembra categoría 5 por la parte frontal.

Los conectores IDC conectan el cable de par trenzado, en la mayoría de los casos por la parte posterior del panel de distribución, aunque algunos fabricantes (como ALCATEL por ejemplo) prefieren que esta conectorización se la realice también por la parte frontal con el fin de facilitar la instalación e intervención. La conexión del cable de par trenzado al conector IDC se la realiza utilizando una herramienta de inserción y corte.

La conectorización con RJ45 está ubicada en la parte frontal del panel de distribución, y son estos conectores los que permiten que los cables

[18] Esta posibilidad debería tratar de descartarse en el diseño original, a menos que la parte económica sea un fuerte limitante.

terminales (*patch cords*) sean fácilmente desconectados y conectados a los equipos del subsistema de conectividad, telefonía, seguridad o control.

B. Paneles de distribución para fibra óptica

Los paneles de distribución para fibra óptica se caracterizan por tener alta densidad de puertos y ser fácilmente instalables para terminar cables de fibra óptica.

Con el mismo criterio que los paneles de distribución para cable de par trenzado, las fibras de cableado horizontal que llegan a los paneles de distribución horizontal o de planta, en su mayoría parten de las salidas de usuario, mientras que para paneles de distribución vertical las fibras llegarán de otros paneles de distribución de planta o de otros paneles de distribución vertical o edificio cuando llegan a un distribuidor de campus. Debe notarse que se habla de cables que llegan a los paneles de distribución; por tanto, a los cables terminales (*patch cords*) que sirven para interconectar los paneles de distribución con los equipos activos del subsistema de conectividad, se los llamará cables salientes de los paneles de distribución.

Los paneles de distribución de fibra óptica también deben ser montables en gabinetes (*racks*) de 19'. Además la mayor parte de fabricantes crean sus paneles con capacidad para 12, 24, 48 y 72 puertos, que por la característica de modularidad permite personalizar casi cualquier instalación.

La amplia gama de paneles de distribución de fibra óptica, por otro lado, permiten casi cualquier variedad de cable de fibra óptica: preconectorizados o sin conectorizar, con empalmes mecánicos o por fusión, monomodales o multimodales, etc. Además pueden adquirirse para utilización con conectores ST, SC, etc.

Para el cableado de fibra óptica es muy importante aunque no obligatorio, la utilización de bandejas (a más de las guías de cableado), que permitan ordenar el cable y principalmente garantizar el radio de curvatura mínimo de las fibras.

2.3.3.6 Bloques de conexión con módulos IDC

Con el fin de reducir costos en la inversión de paneles de distribución para aplicaciones en las que normalmente no se requieren opciones de puenteo en el cableado de par trenzado (en telefonía por ejemplo) se utilizan regletas o bloques de conexión tipo 110 cuya conectorización es de tipo IDC-IDC (Contactos por desplazamiento de aislamiento). Los bloques de conexión están formados por módulos de conexión IDC, que generalmente vienen con una capacidad de 10 pares cada uno.

En la figura 2.41 se muestra un bloque de conexión tipo 110 clásico, el cual requiere de una herramienta de inserción:

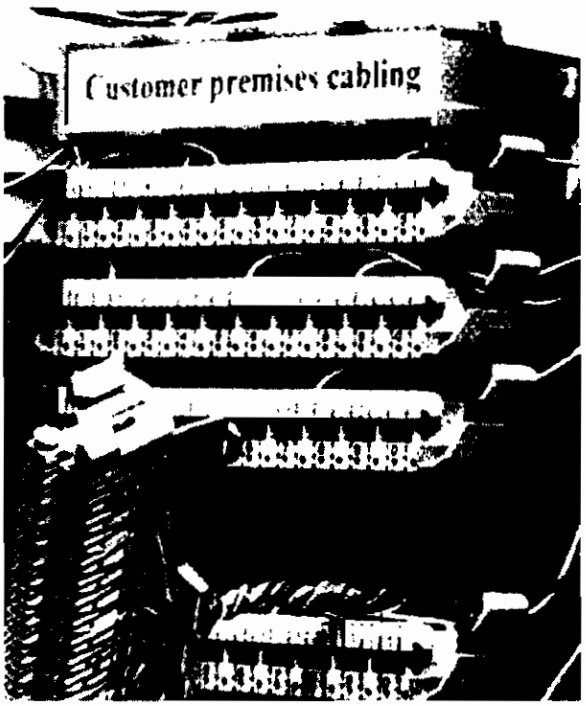


***Figura 2.41* Bloque de conexión tipo 110 (típico)**

En la figura 2.42 se muestra un bloque de conexión 110, cuyos conectores IDC incluyen la característica *Easy Lock* (como la llama IBM), la cual no requiere de herramienta de inserción para la conexión de sus cables:

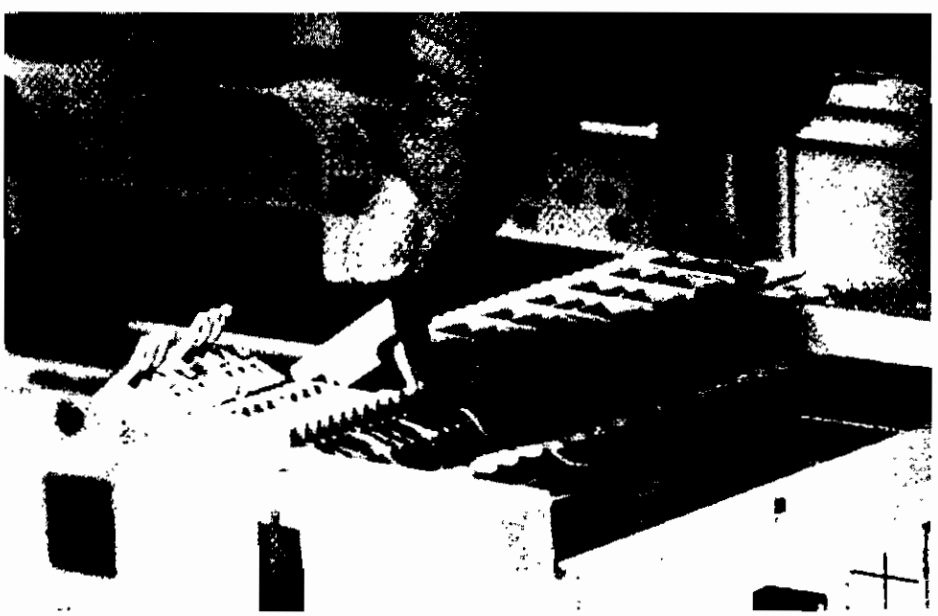


***Figura 2.42* Regleta bloque 110 con herramienta "easy look" integrada**

Los módulos de conexión IDC permiten concentrar en poco espacio una gran cantidad de pares, siendo además de gran modularidad. Otra característica valiosa de estos módulos, es la posibilidad de corte y prueba para la separación de segmentos de línea a la hora del mantenimiento en la red. Debido a la forma en que el cable queda insertado en el conector IDC, es recomendable para conexiones fijas, asegurando de esta manera protección contra vibraciones y cargas de tracción.

2.3.3.7 Gabinetes (*racks*)

Los gabinetes, *racks* o armarios, son la estructura física donde serán montados los paneles de distribución, los equipos activos de conectividad y los bloques de conexión, permitiendo organizar la distribución de cables de tendido (horizontal o vertical) y cables terminales (*patch cords*). Los armarios vienen con un ancho normalizado de 19' y una altura variable, según la necesidad.

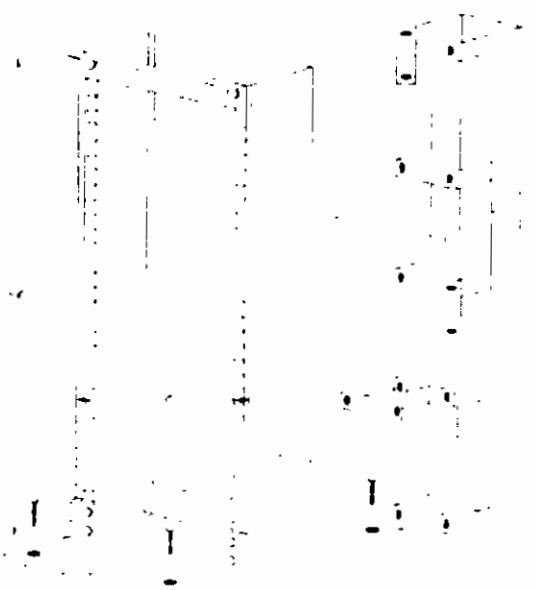


Figura 2.43 RACK con guía de cables sin armario

Además de la estética y la organización de los armarios, es importante que sus cuadros internos y accesorios de montaje, posean una estructura resistente al peso que se coloque sobre ella.

El equipo montado sobre los largueros de 19' debe ser visible (especialmente el equipo activo), mientras que los cables de tendido y terminales pueden ocultarse o estar a la vista. Para combinar esta característica de visualidad con otra importante que es la seguridad, algunos fabricantes han optado por utilizar una puerta delantera de vidrio con marco metálico y cerradura de seguridad.

Normalmente también se tiene acceso por la parte posterior, la cual puede estar dotada con una puerta de seguridad, no necesariamente de vidrio, aunque este acceso podría ser lateral. Algunos fabricantes presentan la opción de armarios que están equipados con cuadros que giran completamente para acceder a la parte posterior de los componentes desde la parte delantera del armario.

Además, los gabinetes pueden equiparse con accesorios como los siguientes: entradas de cables, guías, bandejas, ventiladores, barras de distribución de fuerza, iluminación, puesta a tierra, etc. Para esto, es importante que el tamaño en ancho y profundidad del armario como tal, sea lo suficientemente holgado, para poder instalar y manejar con comodidad y orden tanto el cableado como los accesorios instalados.

En muchos de los casos el suelo de los armarios es hueco, con el propósito de permitir el paso de cable; y el techo, también hueco, normalmente es utilizado para incorporar dispositivos de ventilación.

2.3.3.8 Etiquetado y nomenclatura

El cableado estructurado se debe complementar con un etiquetado claro y duradero. Todos los elementos empleados en la instalación deben etiquetarse convenientemente para facilitar su identificación o reasignación. En general se utilizan etiquetas de papel metalizado autoadherible y de impresión térmica.

Etiquetado de las cajas de conexión. Generalmente se utilizan etiquetas de poliester, con gráficos para la identificación visual de los servicios de voz y datos.

Etiquetado de cables. Generalmente se utilizan etiquetas fabricadas con fluoruro de polivinilo, que soportan temperaturas entre -40°C y 128°C, resistentes al aceite, agua, humedad y disolventes.

Etiquetado de canaletas. Pueden utilizarse las mismas etiquetas que se utilizan para cableado, pero con un tamaño mayor.

Etiquetado en paneles de distribución. Estos elementos pueden utilizar etiquetas de poliéster, montados sobre o debajo de cada una de las conexiones disponibles.

Etiquetado en bloques de conexión con módulos IDC. Se pueden utilizar soportes porta-rótulos reclinables, con protección para el rótulo de papel.

Etiquetado de gabinetes. Pueden utilizarse etiquetas de poliéster, con un tamaño acorde con el tamaño de gabinete.

Es sumamente importante establecer una **nomenclatura** sencilla pero descriptiva, que permita identificar fácilmente los elementos del sistema. Para establecer la nomenclatura, sería aconsejable distribuir el sistema de acuerdo a su ubicación física y a su función de servicio. Así por ejemplo, en un edificio de varios pisos, donde el sistema de cableado estructurado incorporará servicios de voz, datos y control por ejemplo, la nomenclatura que haga una identificación del punto instalado podría ser como sigue:

X - ab - cd - ef

donde:

X: Indicará el tipo de servicio
D para datos
V para voz
C para control
ab: Indicará el número de distribuidor de piso
cd: Indicará el número de *patch panel* o bloque 110 al que corresponde dentro del distribuidor de piso
ef: Indicará el puerto del *patch panel* o bloque 100 al que pertenece

2.3.3.9 Pruebas y documentación[19]

Para las pruebas del sistema, es necesario que se cuente con un probador de secuencia y un equipo probador de redes, que permita hacer una verificación punto por punto del cumplimiento total de las normas del sistema de cableado estructurado.

Deberán hacerse las siguientes verificaciones y mediciones, anotando cada parámetro en un cuadro clasificatorio para su posterior documentación:

- Verificación de secuencia
- Distancia del cable de tendido (desde distribuidor hasta la salida de telecomunicaciones). Verificar que sea menor que 90 m.
- Atenuación medida en cada par
- Otros no indispensables:
  - Resistencia del conductor por par y por unidad de longitud (Ω/Km).
  - Capacitancia mutua de cada par y por unidad de longitud (nF/Km).

Para comprobar el estado de instalación de fibra óptica, se utilizan medidores de potencia y reflectores ópticos de dominio (OTDR).

[19] Más información puede encontrarse en el numeral 2.4.2 titulado "Postevaluación" en este mismo capítulo.

Al final de las pruebas, es importante que se entregue un informe con los resultados obtenidos y si es posible una comparación con las normas de estandarización.

El establecimiento de una correcta documentación del sistema de cableado estructurado, deberá poseer las siguientes partes:

- Tablas que incorporen asignaciones detalladas por cable y que coincidan en nomenclatura con el etiquetado.
- Fórmulas que clarifiquen los criterios tomados en el diseño del sistema de cableado estructurado.
- Diagramas y dibujos que correspondan en nomenclatura a las tablas incorporadas y etiquetado.

Se debe recordar, que la documentación es una herramienta clave para el soporte y mantenimiento que debe darse al sistema de cableado estructurado, por lo que el mantenerla actualizada es la tarea de mayor importancia en esta parte. Actualmente, se cuenta con herramientas de *software* que facilitan la actualización de la documentación tanto escrita como gráfica.

2.4 EVALUACIÓN DE LA INFRAESTRUCTURA DE TRANSPORTE DE UNA RED ESTRUCTURADA DE DATOS

En esta tesis se divide la evaluación de la infraestructura de transporte de una red estructurada de datos en dos partes: la preevaluación y la postevaluación.

La preevaluación se refiere a la evaluación que se recomienda hacer antes de la implementación de la infraestructura de transporte, y hará consideraciones de una infraestructura de telecomunicaciones en general, por lo que algunos de los términos, pese a ser considerados, no serán explicados pues la presente tesis está orientada a las redes de datos. Adicionalmente, la evaluación propuesta utilizará terminología relacionada con tecnología del subsistema de conectividad, básicamente porque la infraestructura de transporte deberá proveer el soporte para que sobre ella se instale cualquier servicio incluido en el subsistema de conectividad. Por esta razón se recomienda referirse al capítulo III de esta tesis como una guía para entender los términos utilizados en esta parte.

La postevaluación se refiere a la evaluación que se recomienda hacer luego de la implementación de la infraestructura de transporte. La postevaluación considera fundamentalmente parámetros cuantitativos que deberán tomarse en cuenta para realizar la calificación de la infraestructura de transporte instalada.

Se puede hablar además de una evaluación durante la implementación, donde se hagan observaciones en cuanto a técnicas de instalación principalmente. Esta evaluación deberá ser realizada por gente con experiencia en instalaciones y con el suficiente

criterio y conocimiento de muchos de los temas que se han expuesto a lo largo de este capítulo en esta tesis y por esta razón no se ha resumido a continuación.

2.4.1 PREEVALUACIÓN[20]

El sistema de cableado Ericsson, presenta una interesante forma de evaluar un sistema de infraestructura de transporte para la preevaluación. Se notará que existe terminología relativa a telefonía y redes WAN, sin embargo estos términos no han sido omitidos aún cuando el tema no corresponde al estudio de la presente tesis. La razón está en mantener las tablas como originalmente fueron diseñadas para que pueda visualizarse el concepto del manejo global de las telecomunicaciones dentro de los sistemas de cableado estructurado.

La evaluación utiliza tablas organizadas para cada una de las siguientes metas, y que fueron presentadas al comienzo de este capítulo: conectividad, flexibilidad, compatibilidad, disponibilidad, capacidad, modularidad y productividad.

2.4.1.1 Conectividad

Esta característica deberá garantizar que la infraestructura de transporte instalada, sea independiente de los requerimientos del departamento, de tal forma que cualquier parte del subsistema, soporte cualquier servicio y aplicación. Todos los cambios que se deban realizar, deben poder efectuarse en un tiempo mínimo.

Entre las características de conectividad que se recomienda evaluar están las mostradas en la tabla 2.19.

2.4.1.2 Flexibilidad

La infraestructura de transporte debería tener una arquitectura abierta la cual no excluya nuevos servicios de comunicación con diferentes velocidades y protocolos.

Entre las características de flexibilidad que se recomienda evaluar están las mostradas en la tabla 2.20.

2.4.1.3 Compatibilidad

Para cada servicio, la infraestructura de transporte debería soportar estándares de interfaz relevantes, y debería asegurar interoperatibilidad del dispositivo para ese servicio.

[20] Tomado del sistema de cableado Ericsson

Entre las características de compatibilidad que se recomienda evaluar están las mostradas en la tabla 2.21.

Características de conectividad
Amplia selección de servicios y protocolos de escritorio • *Token-Ring* 4-16 Mbps • Ethernet 10BaseT, 10Base2, 10Base5 • Conectividad isocrónica T1 y E1 para voz • Video conferencia en Nx64 y Nx56 Kbps • Terminales IBM 3270 con multiplexión de 8 y 32 puertos • Terminales IBM 5250 con multiplexión de 7 puertos • Terminales IBM 5080/6090 con multiplexión de 8 puertos • Terminales RS232 (protocolo transparente) • Conexiones sincrónicas RS-232 y V35 • Otras
Amplia selección del medio horizontal • UTP para todos los protocolos • STP para todos los protocolos • Coaxial y twinaxial para protocolos relevantes • Conectores por puerto
Facilidad del cambio de servicio en la salida • Nivel de personal técnico requerido • Tiempo requerido para efectuar el cambio
Posibilidad de cambios sin afectar el servicio • Puertos de soporte adicional para servicios existentes • Servicios y protocolos de soporte adicional
Habilitación/Deshabilitación desde consola de administración • Puertos para usuarios individuales • Módulos para crear redes virtuales adicionales • Cargas balanceadas para LANS
Ancho de banda del *backbone* (100 MHz) • Ahorro de ancho de banda para bajos costos y cambios rápidos
Selección del medio de fibra óptica para *backbone* • 62.5/125 µm multimodo (fibra estándar) • 50/125 µm multimodo • 9/125 µm monomodo (para redes en campus o área metropolitana)

***Tabla 2.19** Características para evaluación de conectividad que debería soportar una infraestructura de transporte*

Característica de flexibilidad
Arquitectura de red virtual • Conectividad de bit transparente con demora insignificante • Soporta y distribuye sincronización WAN de 8 KHz • Buffers de latencia multiprogramables • Compatible con estándar SONET/SDH
Topología de *backbone* colapsado • Migración simplificada a nuevos protocolos • Soporte estable para red física y de fácil reconfiguración • Elimina cuellos de botella de interconectividad en armarios
Soporta video-conferencia y multimedia • Arquitectura compatible con ISO Ethernet • Arquitectura compatible con ATM • Segmentación simple de LAN fuera de servicio a un único usuario • Compatibilidad ISDN/PRI en E1 y T1 • Arquitectura compatible con ISDN/BRI
Software de hub descargable • Elimina costos y permite actualizaciones de PROM • Fácil adición de nuevas características de conectividad • Mantiene su lugar con la evolución en estándares de administración • Puede descargarse a través de módem o directamente desde un PC

Tabla 2.20 Características para evaluación de flexibilidad que debería soportar una infraestructura de transporte

Característica de compatibilidad
EIA-TIA/568 *Commercial Building Telecommunications Wiring Standard*
IAB-RFC1157A *Simple Network Management Protocol* (SNMP)
IAB-RFC1213 *Management Information Base for Network Management of TCP/IP-based interfaces*: MIB-II
IAB-RFC 1271 *Remote Network Monitoring Management Information Base* (RMON)
IEEE 802.3 Método de acceso CSMA/CD y especificaciones de capa física
IEEE 802.5 Método de acceso *Token-Ring* y especificaciones de capa física
ANSI E1.10X Especificaciones de red digital
CCITT G.703 Característica físicas/eléctricas de interfaces digitales jerárquicos
CCITT G.704 Características funcionales de interfaces asociados con nodos de red
CCITT V.35 Interfaz para módem de banda amplia
EIA-TIA-232-E Interfaz entre DTE y DCE empleando interfaz serial de datos binarios
IBM/3270PAI Información para enlazar la unidad de control al dispositivo
IBM/5250PAI Información para enlazar IDS a S/36, S/38 y AS400
IBM/5280PAI Información para enlazar controlador de canal 5088 a procesador IBM 5085
Bellcore/TR-TSY-000499 Requerimientos genéricos del sistema de transporte: requerimientos comunes
Bellcore/TR-TSY-000253 Sistema de transporte SONET: criterio genérico común

Tabla 2.21 Características para evaluación de compatibilidad que debería soportar una infraestructura de transporte

2.4.1.4 Disponibilidad

El tiempo que la infraestructura de transporte debe estar disponible a ser usada, debe ser el máximo posible. Ericsson recomienda que el tiempo fuera de servicio para ambientes normales, debería ser menor a una hora por año, y que para ambientes críticos de servicio, este tiempo *debería* ser menor a 6 minutos por año.

Entre las características de disponibilidad que se recomienda evaluar están las mostradas en la tabla 2.22.

Característica de disponibilidad
Diseño de *hardware* confiable • Módulos completamente cerrados sin exponer circuitos electrónicos • 25 años MTBF para módulos de control • 40 a 200 años MTBF para módulos de acceso • Opción de fuente de poder redundante • Opción de módulo de control completamente redundante
Configuración confiable de la red • Anillos redundantes eliminan fallas en un anillo simple • Topología dual en estrella soporta caminos redundantes • Redes de supervivencia para recuperación de desastres • *Backbone* colapsado simplifica aislar fallas
Control de administración de la red • Segmentación manual y automática de puertos con falla • Segmentación manual y automática de módulos con falla • Reportes de eventos de ingreso y alarma

***Tabla 2.22** Características para evaluación de disponibilidad que debería soportar una infraestructura de transporte*

2.4.1.5 Capacidad

Características de capacidad
Topología del *backbone* colapsado • Capacidad total de la red escalable con número de armarios • Grandes redes escalables a múltiple capacidad Gbps • Capacidad de 100 Mbps en cada hub/armario
Tecnología de *backbone* multiplexado • 100 Mbps por par de fibra • Hasta 8 redes virtuales por hub • Hasta 32 redes virtuales por par de segmento/fibra

***Tabla 2.23** Características para evaluación de capacidad que debería soportar una infraestructura de transporte*

Una infraestructura de transporte bien diseñada, debería poder acomodar requerimientos de capacidad anticipada para un período de 5 años, según la empresa de telecomunicaciones Ericsson. Debe notarse que la mayoría de fabricantes ofrecen una garantía de 15 años en calidad, no en capacidad.

Entre las características de capacidad que se recomienda evaluar están las mostradas en la tabla 2.23.

2.4.1.6 Modularidad

Una infraestructura de transporte debe utilizar elementos de diseño modular, que permitan un crecimiento con elementos homogéneos y que funcionen en armonía. Es decir *deberían* permitir un diseño a futuro sin necesariamente hacer la compra inicial total de las partes, pero es importante que las partes compradas pertenezcan a una empresa que tenga una trayectoria considerable para garantizar la provisión de partes y repuestos en el futuro.

Entre las características de modularidad que se recomienda evaluar están las mostradas en la tabla 2.24.

Características de modularidad
Cajas modulares totalmente pasivas (proveen mejor modularidad)
Módulos compatibles con caja modular
Tiempo que fábrica garantiza creación de módulos para determinado modelo de caja modular
Años de servicio de empresa proveedora en el ámbito internacional
Años de servicio de empresa proveedora en el ámbito nacional
Experiencia anterior con empresa proveedora
Experiencia de otras empresas con empresa proveedora

Tabla 2.24 Características para evaluación de modularidad que debería soportar una infraestructura de transporte

2.4.1.7 Productividad

La productividad incluye todo el equipo, costos de instalación, entrenamiento, mantenimiento, cambio y tiempo fuera de servicio durante la vida útil de la infraestructura de transporte.

Entre las características de productividad que se recomienda evaluar están las mostradas en la tabla 2.25.

Características de productividad
Infraestructura simple • Para datos, voz y video • Costos reducidos de administración, equipamiento y espacio
Bajo costo de instalación • Mínimo espacio requerido de 2'x2' en la pared • Equipamiento con 6' de profundidad permite la instalación en pequeños gabinetes • Tasa de instalación excede los 30 usuarios por hombre-hora
Bajo costo de administración y mantenimiento • Un administrador de red por cada 2500 puertos de red
Costo de tiempo fuera de servicio • Menos que 1/10 hora promedio de tiempo fuera de servicio por año para usuarios enlazados a un sistema redundante (99.999% de disponibilidad) • Menos que 1 hora promedio de tiempo fuera de servicio por año para usuarios enlazados a un sistema no redundante (99.99% de disponibilidad)
Arquitectura de *backbone* colapsado • Costo reducido de equipo de interconectividad • Costo reducido del sistema de administración
Bajo costo de equipamiento • Precio de compra inicial • Garantía y reparación

***Tabla 2.25** Características para evaluación de productividad que debería soportar una infraestructura de transporte*

2.4.2 POSTEVALUACIÓN

La postevaluación se refiere fundamentalmente al levantamiento de parámetros cuantitativos que certifiquen la infraestructura de transporte estructurada instalada.

Para este proceso será necesario utilizar equipo que permita medir los mencionados parámetros. Entre los instrumentos utilizados, están principalmente un probador de secuencia y un equipo de prueba para redes LAN-TESTER. Con este equipo se realizará las mediciones necesarias para verificar punto a punto el cumplimiento total de las normas de cableado estructurado.

Entre los parámetros a medir que tienen mayor importancia están: verificación de continuidad y secuencia, la longitud de los cables de tendido, y la atenuación. Otros parámetros a considerar serán la diafonía, NEXT, capacitancia y resistividad por unidad de longitud, etc.

2.4.2.1 Verificación de secuencia y continuidad

Para la verificación de secuencia y continuidad se utiliza el Probador de secuencia que posee una unidad principal y una remota. Se coloca la unidad principal o generadora

de señal en uno de los extremos y la unidad remota en el otro. El probador se encargará de indicarnos si el secuenciamiento utilizado es el correcto de acuerdo a la norma seleccionada, y si todos los pares del cable están salvos de rotura (continuidad).

2.4.2.2 Longitud

Esta prueba se la realiza utilizando un probador de redes que mida la longitud del cable mediante procedimientos indicados en este mismo capítulo. Según las normas ANSI/EIA/TIA ninguno de los cables de tendido horizontal entre el SDF (distribuidor de piso o *closet* de telecomunicaciones) hasta el área de trabajo (*wall plate* o salida de telecomunicaciones) debe exceder los 90 m.

2.4.2.3 Atenuación

La pérdida de amplitud de la señal a lo largo del cable (atenuación) se mide en cada uno de los pares inyectando en uno de los extremos una señal a una frecuencia entre 5 y 100 MHz (para cable UTP categoría 5) y se detecta la señal con otro dispositivo (*scanner*) en el otro extremo. El *scanner* mide la amplitud de la onda recibida y determina por diferencia la atenuación, desplegando en la pantalla su valor en decibelios.

Debe acotarse, que los valores de atenuación permitidos están determinados en cada una de las normas del estándar de red correspondiente, por ejemplo para la norma IEEE 802.3 sobre cable UTP (10BaseT) los rangos de atenuación para cualquiera de los dos pares utilizados es de máximo -11.5 dB. Algunos valores que se obtienen comúnmente en las pruebas se muestran en la tabla 2.17 "Especificaciones de cable de par trenzado" de este mismo capítulo.

Finalmente, es importante recordar que cada uno de estos parámetros debe ser registrado en las tablas de pruebas que se adjuntan con la documentación del sistema de cableado estructurado.

2.5 ADMINISTRACIÓN DE LA INFRAESTRUCTURA DE TRANSPORTE DE UNA RED ESTRUCTURADA DE DATOS

Es bueno recordar que la tecnología crece en función de necesidades y de objetivos que brinden mayores comodidades y facilidades en el trabajo con dicha tecnología, que la haga cada vez más independiente del ser humano, teniendo como meta ideal: "la tecnología al servicio del hombre pero independiente de él".

La administración de la tecnología en general, es uno de los aspectos que más fortalece esta dependencia, por esta razón, en los últimos años está siendo tratada como uno de los aspectos de mayor importancia, y seguramente, en un futuro no muy lejano,

la propia tecnología será quien se encargue de autoadministrarse a costos accesibles a la mayoría de entidades.

El sistema de cableado estructurado, por sí mismo, es un sistema estructurado que posiblemente se concibió de la necesidad de crear infraestructuras de transporte estructuradas que sean más fáciles de administrar. Por esta razón, y como se mencionó anteriormente en este capítulo, la infraestructura de transporte estructurada que tendrá mayor cabida en un futuro no muy lejano será seguramente aquella que no utilice cable como medio de transmisión.

Si se hace un análisis rápido de lo que es un sistema estructurado, es casi tácita la relación que tiene la palabra "estructurado" con la palabra "ordenado" y por tanto con la frase "fácil de administrar".

El propósito de administrar la infraestructura de transporte de una red estructurada de datos, es proveer un esquema de administración uniforme para la infraestructura de telecomunicaciones que sea independiente de los sistemas de comunicaciones específicos que operan sobre la mencionada infraestructura.

De la bibliografía que se ha revisado sobre temas relacionados a la presente tesis, no se dedican muchas líneas a la administración de la infraestructura de transporte, aunque si se lo hace para el subsistema de conectividad. En general, la mayoría de autores han concebido la administración de una red de datos como la administración de lo que puede considerarse la "parte activa" de la mencionada red, dedicando muy poco a la administración de la "parte pasiva".

Por esta razón, a la administración de la infraestructura de transporte de una red estructurada de datos, se la tratará en función de las recomendaciones que hace el estándar ANSI/EIA/TIA-606 "Administration Standard for the Telecommunications Infraestructure of Commercial Buildings". Considerando que la infraestructura de transporte de una red estructurada de datos actual está concebida dentro de lo que es un sistema de cableado estructurado, el estándar ANSI/EIA/TIA-606 es el documento que mejor orienta la administración de una infraestructura de transporte de datos actual.

Debe notarse que el estándar ANSI/EIA/TIA-606 está enfocado a la administración de una infraestructura de telecomunicaciones en general, donde están incluidos los datos. En referencia a la última aclaración, se debe observar que la diferencia entre sistemas de datos y sistemas de telecomunicaciones al menos en edificios comerciales, cada vez es más pequeña.

La información que será provista a continuación ha sido adaptada del estándar ANSI/EIA/TIA-606. La presente tesis no garantiza la exactitud, aplicabilidad, o interpretación de esta información; para detalles completos debe consultarse el mencionado estándar.

2.5.1 ANSI/EIA/TIA-606, ADMINISTRATION STANDARD FOR THE TELECOMMUNICATIONS INFRAESTRUCTURE OF COMMERCIAL BUILDINGS

2.5.1.1 Propósito y alcance

El propósito del estándar ANSI/EIA/TIA-606 es proveer un esquema de administración uniforme para la infraestructura de telecomunicaciones (infraestructura de transporte) que es independiente del sistema de comunicaciones (subsistema de conectividad) específico que opera sobre la mencionada infraestructura.

El estándar comprende espacios (*spaces*), canaletas para cable (*cable pathways*), conexión a tierra (*grounding*), cableado (*wiring*), y *hardware* de terminación (*termination hardware*).

El estándar no incluye la administración del equipo de usuario final en las áreas de trabajo, tampoco incluye ningún equipo perteneciente al subsistema de conectividad (tales como *hubs*, controladores, multiplexores, etc).

En el estándar se presentan muchos ejemplos e ilustraciones que no son cubiertos en esta tesis.

2.5.1.2 Conceptos Generales

El esquema de administración definido por el estándar ANSI/EIA/TIA-606 básicamente envuelve aspectos de documentación tales como etiquetas, registros (*records*), dibujos (*drawings*), reportes (*reports*), y órdenes de trabajo (*work orders*).

Como en el resto de estándares, se presentan partes mandatorias del estándar que se encargan de especificar los requerimientos mínimos aceptables, mientras que las partes de advertencia son recomendaciones opcionales las cuales podrían mejorar el rendimiento y beneficio a usuarios.

Para cada elemento de infraestructura (tipo de elemento), el estándar especifica identificadores requeridos (*required identifiers*), atributos (*attributes*) y eslabones (*linkages*). Un identificador es el único nombre de elemento particular, mientras que un atributo es una propiedad de un elemento particular. Un identificador y sus atributos relativos son un registro. Una lista de registros para un elemento particular es una tabla. Un eslabón representa una única relación entre dos elementos.

El usuario es el responsable de crear su propia nomenclatura (convenciones de nombre) para identificadores y atributos. El estándar no especifica normas de longitud ni de formato.

2.5.1.3 Elementos y documentación

En numerales anteriores de este capítulo han sido tratados los elementos de una infraestructura de transporte estructurada. Sin embargo es interesante conocer la forma en que el estándar ANSI/EIA/TIA-606 hace referencia a los elementos de un sistema de cableado estructurado, y a la información requerida que debe recogerse y grabarse sobre dichos elementos, con el objeto de mantener un sistema documentado.

Considerando que el estándar debe ser la guía para la administración de cableado estructurado, en esta tesis se ha realizado un pequeño resumen de los elementos y documentación del estándar original. Este resumen se presenta en la parte de anexos titulado como "Resumen de elementos y documentación de un sistema de cableado estructurado según el estándar ANSI/EIA/TIA-606 para la administración de redes estructuradas".

2.5.1.4 Etiquetado

Las reglas para la etiquetación están basadas en requerimientos establecidos en ANSI/EIA/TIA-568-A, 569, y 607.

Las etiquetas están clasificadas como adhesivas, de inserción u otros tipos tales como etiquetas tie-on (de unión). Todas las etiquetas deben cumplir los requerimientos de legibilidad, estropeo, adhesión y exposición como se especifica en UL 969.

Las etiquetas autolaminadas son recomendadas para etiquetación de los cables más pequeños. Las etiquetas siempre deben ser visibles.

Si la cubierta de un dispositivo está hecha para ser etiquetada, la cubierta debe permanecer sujeta o asociada con el dispositivo.

El código de barras sobre etiquetas debe estar de acuerdo a USS-39 (también llamado código 39) o USS-128 (también llamado código 128). Todas las etiquetas de código de barras deben tener impreso el identificador.

2.5.1.5 Codificación de colores para etiquetas

El uso de codificación de colores en la etiquetación es requerido para todas las terminaciones de cable. Las etiquetas de terminación en cada extremo deben ser del mismo código de color.

El estándar permite el uso de un código de color mejorado u otros sugeridos por el mercado para designar la categoría de un cable (C3, C4 o C5).

Los códigos de colores especificados son los siguientes:

COLOR	*TIPO DE TERMINACION*	*COMENTARIOS*
Naranja	Punto de demarcación	Terminación de la oficina central, Alimentación de llegada o cables truncados
Verde	Conexión de red	Conexiones de red o terminación de circuito auxiliar
Púrpura	Equipo común tal como PBX, *Host* CPU, Multiplexores	Para todas las terminaciones de equipos de datos y conmutadores principales
Blanco	Primer nivel de los cables del *backbone*	Para el cable de *backbone* entre la conexión de cruce principal (MC) y el *closet* de telecomunicaciones (TC)
Gris	Segundo nivel de los cables de *backbone*	Para los cables de *backbones* entre la conexión de cruce intermedia (IC) y el *closet* de telecomunicaciones (TC)
Azul	Estación	Para terminaciones de cable horizontal
Café	Cable de *backbone* entre edificios	Para las terminaciones de cable de *backbone* de campus
Amarillo	Misceláneo	Para auxiliares, mantenimiento, alarmas, seguridad, etc
Rojo	Sistemas de teléfonos	Para todos las terminaciones de equipo telefónico

***Tabla 2.26** Códigos de colores especificados en la etiquetación de cableado*

Capítulo III

Subsistema de conectividad de una red estructurada de datos, evaluación y administración

III. SUBSISTEMA DE CONECTIVIDAD DE UNA RED ESTRUCTURADA DE DATOS, EVALUACION Y ADMINISTRACION

3.1 INTRODUCCION

Dentro del sistema de red estructurado propuesto, este capítulo trata sobre el *"subsistema de conectividad"*.

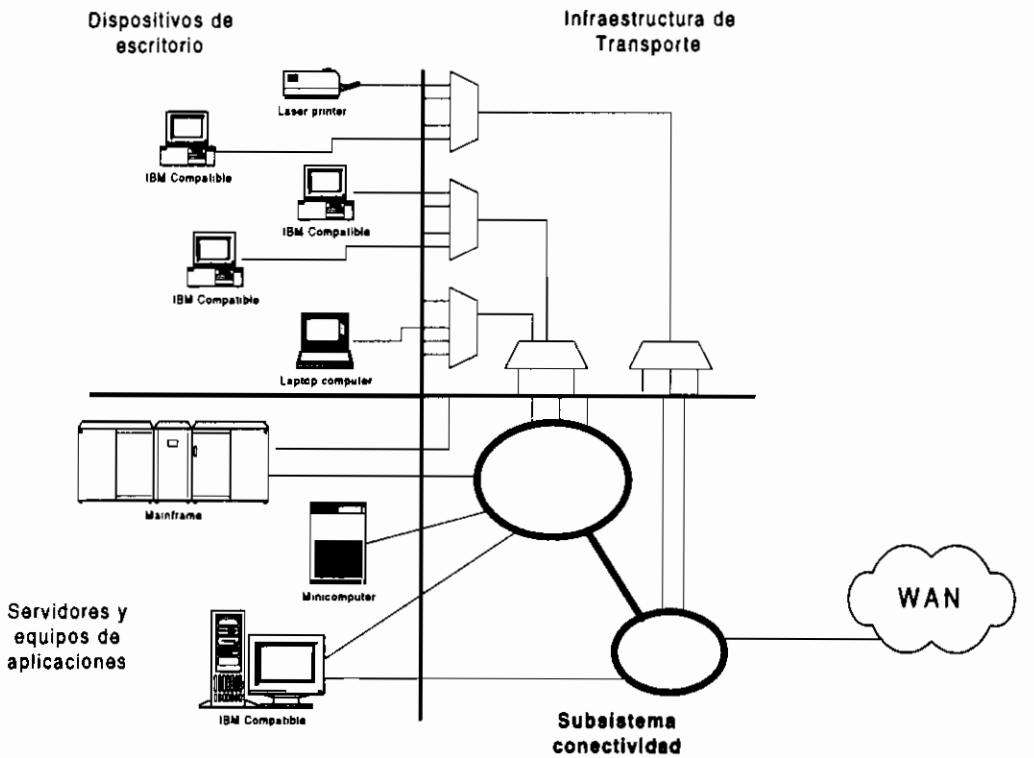


***Figura 3.1** Ubicación del subsistema de conectividad dentro de una red estructurada de datos*

El subsistema de conectividad debe entenderse como el conjunto de elementos activos que proporcionan las funciones necesarias para la utilización de protocolos de comunicación a través de la infraestructura de transporte.

Como se mencionó en el capítulo I, debe diferenciarse entre el camino que permite la comunicación, y los protocolos de comunicación que son las normas que rigen "el idioma y la gramática" que utilizarán los equipos de conectividad. El camino comprende la infraestructura de transporte, mientras que las funciones que permiten la utilización de protocolos de comunicación estarán contenidas dentro del subsistema de conectividad. Está por demás aclarar que ninguno de los subsistemas puede garantizar la comunicación independientemente.

Debido a que actualmente la infraestructura de transporte normalizada internacionalmente es el cableado estructurado, es importante que el subsistema de conectividad mantenga la actualidad y compatibilidad con las normas que rigen los dos subsistemas en conjunto. Además, debe considerarse que los equipos que forman parte del subsistema de conectividad, deberán ser de marcas garantizadas y probadas en el medio, de tal forma que puedan proveer una respuesta técnica adecuada y una trayectoria continua en cuanto a provisión de repuestos y equipos, asegurando de esta forma su permanencia en el mercado nacional e internacional.

En cuanto a características generales, es importante que los equipos utilizados en el subsistema de conectividad cumplan con lo siguiente:

- Tecnología actual
- Alta confiabilidad
- Crecimiento modular
- Sistemas redundantes
- Servicio de mantenimiento en línea sin desconexión previa
- Administrables por medio de *software* básico tipo SNMP[22] como mínimo, y adaptables a otros sistemas de administración en forma opcional y modular
- Montables en racks de 19 pulgadas según normas

3.2 SUBSISTEMA DE CONECTIVIDAD DE UNA RED ESTRUCTURADA DE DATOS Y SU RELACION CON EL MODELO OSI

3.2.1 RELACION CON EL MODELO OSI

El subsistema de conectividad está relacionado principalmente con las tres primeras capas del modelo de referencia OSI.

3.2.2 ELEMENTOS DEL SUBSISTEMA DE CONECTIVIDAD

Los elementos más comunes del subsistema de conectividad son los siguientes:

1. Tarjetas de red
2. *Hubs* o concentradores
3. *Bridges* o puentes
4. *Switches* o conmutadores
5. Ruteadores

[22] SNMP (Simple Network Management Protocol) es un protocolo utilizado en administración de redes.

3.2.2.1 Tarjetas interfaz de red

Las tarjetas de interfaz de red están directamente relacionadas con el nivel físico del modelo de referencia OSI, y técnicamente, una tarjeta de interfaz de red incluye todas las conexiones físicas y lógicas entre el computador, u otro dispositivo y el medio de transmisión. Se trata de una tarjeta lógica que se instala en un computador para conectarlo a un conector de cable.

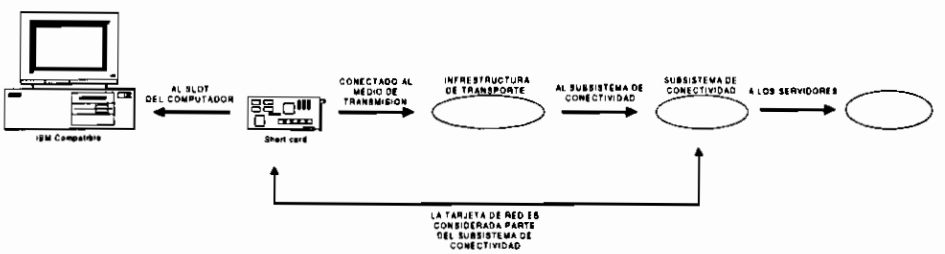


***Figura 3.2** Conexión de una tarjeta de red*

Una tarjeta de red es la interfaz que permite que un computador pueda comunicarse con otros a través de la infraestructura de transporte y subsistema de conectividad.

Estos interfaces incluyen la circuitería y conexiones mecánicas para convertir las señales eléctricas del computador en las señales eléctricas o electromagnéticas que se utilizan en el medio. Una tarjeta suele incluir un solo transceptor[23], pero puede proporcionar uno o más tipos de conector. Cuando se requiera, puede utilizarse un adaptador de medio[24], el cual se encargará de recibir señales en un tipo de conector y convertirlas a otro tipo de conector.

3.2.2.2 *Hubs* o concentradores

Las redes necesitan un punto central de conexión entre los segmentos del medio. Estos puntos se denominan *hubs* o concentradores. Estos dispositivos son una especie de repetidores especiales que superan las limitaciones electromecánicas del único recorrido del medio.

El concentrador se encarga de transmitir las señales entrantes a los restantes segmentos del medio. Fundamentalmente se encuentran tres tipos de concentradores en el mercado:

a. Pasivos
b. Activos
c. Inteligentes

[23] Los transceptores son dispositivos que pueden transmitir y recibir señales eléctricas o electromagnéticas por el medio de transmisión. Algunas transmisiones utilizan LED, diodos N intrínsecos P y fotodiodos de avalancha.

[24] Recordemos que los adaptadores de medio son elementos pertenecientes al subsistema de infraestructura de transporte.

A. Concentradores pasivos

Este tipo de concentradores no llevan a cabo ningún tipo de regeneración de la señal, de tal forma que cada segmento se puede alargar solo a la mitad de la distancia efectiva máxima. Además, cada computador recibe señales que se envían desde otros computadores.

B. Concentradores activos

Es muy semejante al concentrador pasivo, con la excepción que regenera las señales. Por lo tanto, este tipo de concetradores permite que se sobrepase la longitud máxima del cable. El principal inconveniente es que algunos concentradores de este tipo amplifican también el ruido que se introduce con la señal. Todos los computadores siguen recibiendo señales del resto de computadores.

C. Concentradores inteligentes

Estos concentradores (incluyendo los concentradores de conmutación), además de regenerar la señal y permitir gestión de la red, realizan también actividades como selección inteligente de recorrido. Esta capacidad de conmutación, permite que cada segmento sea utilizado sólo cuando se dirija una señal a un computador que se encuentre en ese segmento.

3.2.2.3 *Bridges* o puentes

Los *bridges* son dispositivos que operan en la capa enlace de datos. Se encargan de conectar dos segmentos de red juntos y envían tramas entre segmentos de acuerdo a sus direcciones MAC.

Existen muchas razones para utilizar *bridges* como dispositivos dentro de redes locales y en grandes empresas. Estas razones pueden ser el resultado de limitaciones físicas y/ó razones de mejoramiento de la red. Las razones para la aplicación común de puentes incluyen las siguientes:

- La población de nodos excede las especificaciones máximas
- La necesidad de conectar dos o más sitios remotos
- La necesidad de aislar LANs en plantas o departamentos de un edificio de los sistemas de *backbone* comunes
- Mejoras en la administración de la red
- Interconectividad de grandes empresas

Así por ejemplo, las LANs IEEE 802.3 CSMA/CD e IEEE 802.5 *Token-Ring* tienen un número máximo permitido de dispositivos por LAN, basados en especificaciones físicas. Un sistema LAN IEEE 802.3 puede tener un máximo de 1024

dispositivos direccionables, mientras que IEEE 802.5 *Token-Ring* puede tener 72 dispositivos direccionables para cable UTP y 256 si se utiliza STP.

La segmentación de redes es una de las aplicaciones más utilizada del *bridge*. Para muchas organizaciones, la implementación de un *backbone* de red a través de edificios enteros o campus, permite la integración del sistema de información. El aislamiento del tráfico de red localizada, es un paso importante que es crítico para soportar crecimientos futuros y para mantener un rendimiento óptimo. Cuando los *bridges* segmentan LANs departamentales, el tráfico de la red permanece local al departamento.

Los *backbone* de redes son mejor empleados para transportar tráfico interdepartamental o para proveer conectividad a recursos compartidos y otros sistemas de *host*. Las LANs departamentales pueden interconectarse al *backbone* por medio de un *bridge*.

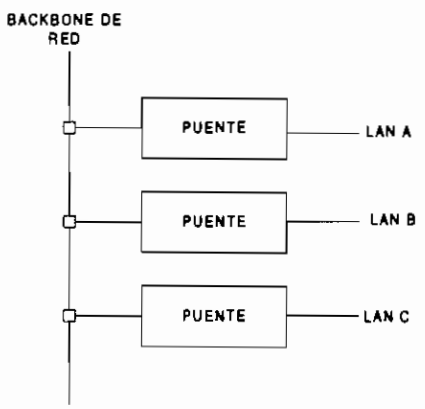


***Figura 3.3** Utilización de puentes para la conexión al backbone*

Muchas redes incluyen *bridges* en los distribuidores de piso (SDF - *Secondary Distribution Frame*) para interconectividad con el *backbone*.

Si bien la presente tesis está orientada a redes de área local, es importante conocer que los puentes o *bridges*, son también utilizados para enlazar LANs remotas, utilizando un par de *bridges*, los cuales funcionan como si ellos estuvieran juntos el uno con el otro. Un enlace de puentes remoto provee una conexión transparente entre LANs.

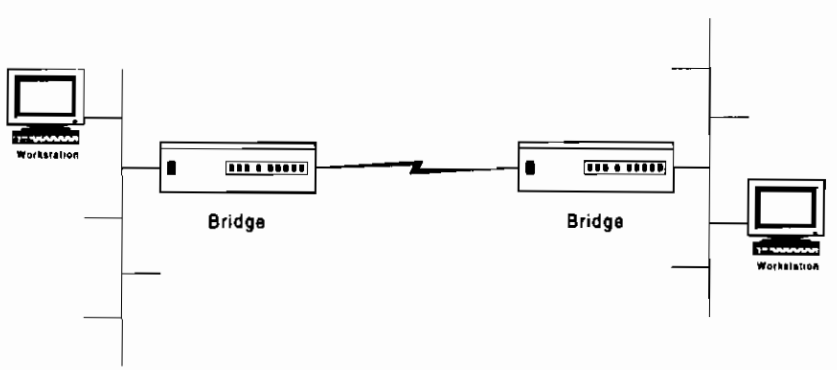


***Figura 3.4** Conexión de LANs utilizando puentes*

A. Arquitectura de un puente

Cada puerto del puente es capaz de transmitir y recibir tramas hacia y desde la LAN a la cual está conectada. Cada puerto del puente posee tres unidades:

1. La unidad de **servicio MAC** maneja todas las funciones de la capa MAC. Aquí son examinadas las direcciones MAC individuales o de grupo que están asociadas al puerto.
2. La unidad de **MAC Relay** maneja las retransmisiones de las tramas entre los pórticos del puente, tramas filtradas y aprendizaje de la información de filtración de tramas.
3. La unidad **protocolo del puente (*bridge*)** es utilizada para el algoritmo de árbol de cruce (*Spanning tree*) y protocolo responsable de la configuración de la topología del puente dentro de la red. La unidad protocolo del puente entre puentes, comunica el uno con el otro utilizando *Bridge Protocol Data Unit (BPDU).*

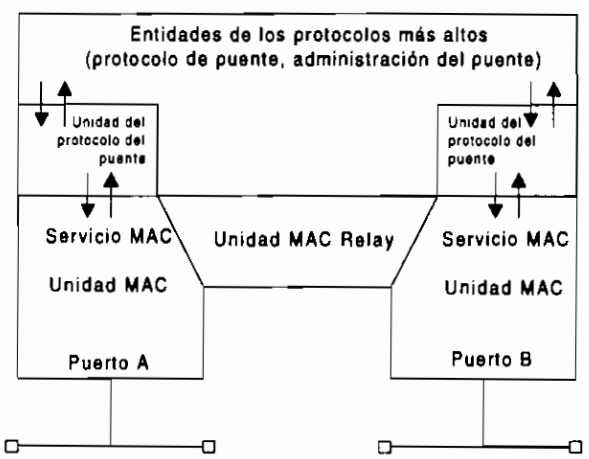


***Figura 3.5** Arquitectura de un puente*

B. Operación de un puente

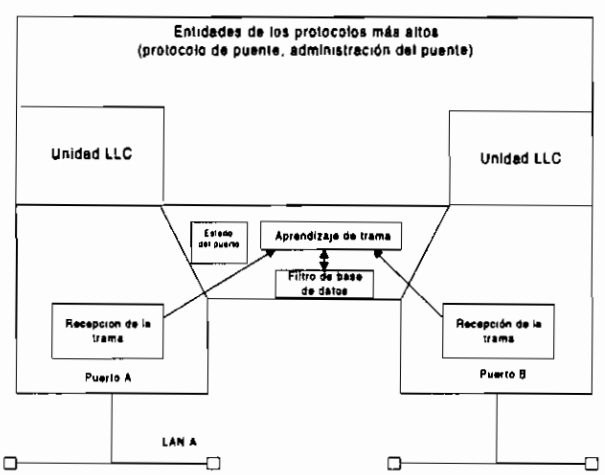


***Figura 3.6** Operación de un puente*

A continuación se describe la operación de un puente para la capa MAC (ver figura 3.6):

- El **Proceso de aprendizaje o Proceso de escucha,** es donde cada pórtico del *bridge* observa la dirección fuente de cada trama recibida y actualiza la base de datos de filtración, basada en el pórtico que recibió la trama.
- El **Proceso de envío/filtración** envía las tramas recibidas que van a ser reenviadas a otros pórticos del puente basado en la información contenida en la base de datos de filtración.

La información del estado del pórtico especifica cuando el puerto de un *bridge* está en modo de aprendizaje, modo de filtrado o modo de envío.

B.1 Proceso de aprendizaje

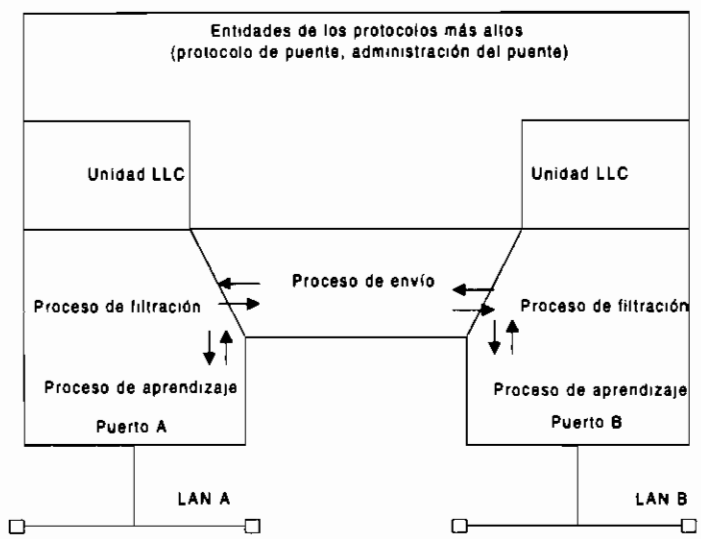


Figura 3.7 Proceso de aprendizaje

En el proceso de aprendizaje se examinan cada una de las direcciones fuente de las tramas y se graban las direcciones en la base de datos de filtración. Cada una de las direcciones fuente, es actualizada a la base de datos de filtración si y solamente si las siguientes condiciones ocurren:

- El pórtico sobre el cual la trama fue recibida está en un estado que permite el aprendizaje.
- El campo de dirección fuente de la trama denota un único nodo final y no es un grupo de direcciones.
- Una entrada estática para la dirección MAC asociada no está lista.
- El número resultante de entradas no excede la capacidad de la base de datos de filtración. (Más bases de datos de filtración permiten nuevas entradas para sobreescribir a las más viejas - FIFO).

B.2 Proceso de envío

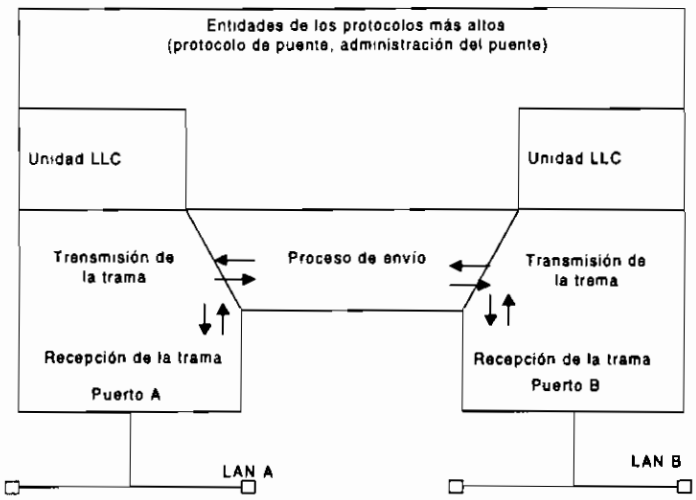


Figura 3.8 Proceso de envío

Las funciones del proceso de envío de un puente en la capa MAC son (ver figura 3.8):

1. Se determina la información del estado del pórtico para establecer el modo de envío tanto para el pórtico sobre el cual la trama fue recibida y el pórtico al cual la trama será transmitida.
2. Se cumple la recepción de la trama al someter a la unidad de servicios MAC todas las tramas válidas.
3. Se cumple la transmisión de tramas por la unidad de servicios MAC dentro de cada pórtico del puente. Las tramas retransmitidas son sometidas para transmisión por el proceso de envío.
4. En el proceso de envío de tramas, se envían tramas que son retransmitidas a otros pórticos del puente. Las tramas son filtradas considerando si la dirección de destino es contenida en la base de datos de filtración o no, y dependiendo si el máximo tamaño de la unidad de datos que es soportada por la LAN a la cual el pórtico de transmisión está conectado no está excedido.

El proceso de envío también provee almacenamiento para tramas en cola de espera. El esquema de orden FIFO debería ser mantenido con los puentes de la capa MAC. Las tramas pueden ser removidas de la cola (por ejemplo un *buffer* de memoria) por el proceso de envío si una de las siguientes condiciones se garantiza:

- Si el tiempo para el cual el almacenamiento temporal (*buffer*ing) ha sido excedido (por ejemplo si la trama es atrapada en la cola por demasiado tiempo).
- Si es necesario asegurar que la máxima demora de transmisión del puente no debería ser excedida (por ejemplo un cuello de botella se ha producido)
- Si el puerto asociado deja el estado de envío.

B.3 Proceso de filtración

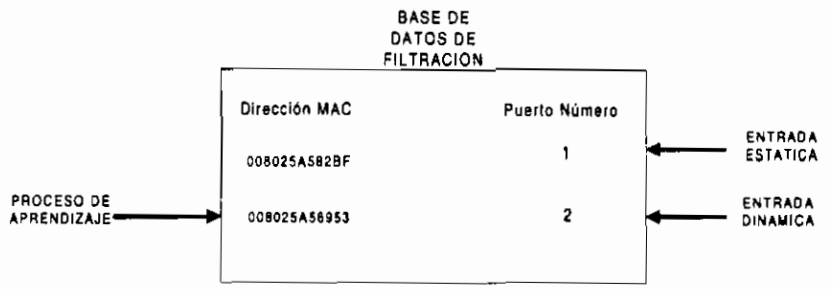


***Figura 3.9** Base de datos de filtración*

Los requerimientos de envío son verificados contra la base de datos de filtración. La base de datos de filtración retiene la información de filtrado que fue explícitamente configurada o que ingresó automáticamente por el proceso de aprendizaje. La mayoría de sistemas de administración permiten que la base de datos de filtración sea examinada. La base de datos de filtración debería ser capaz de contener entradas estáticas o dinámicas de acuerdo a lo siguiente:

- Las **entradas estáticas** podrían ser añadidas o borradas por un control de administración específico. Las entradas estáticas especifican las direcciones MAC para las cuales la filtración es especificada y proveen un mapa de pórtico que especifica cuales tramas podrían y cuales no podrían ser transmitidas a ese pórtico.
- Las **entradas dinámicas** son creadas y actualizadas transparentemente por el proceso de aprendizaje. Las entradas dinámicas especifican las direcciones MAC para las cuales el filtrado es especificado y el número de puerto designado para el cual fue aprendido. Las entradas dinámicas son típicamente removidas de la base de datos de filtración después de una cantidad específica de tiempo, llamada tiempo fuera *(Time-Out o Aging Time).* Este tiempo, asegura que los nodos de la estación que han sido removidos a diferentes partes de la red no serán permanentemente prevenidos de las tramas recibidas.

C. Tipos de puentes

C.1 Puentes transparentes

Los puentes transparentes pueden ser implementados para IEEE 802.3 CSMA/CD o IEEE 802.5. Los puentes transparentes tienen las siguientes características:

- Utilizados para conexión de redes locales LAN-a-LAN
- No separan las redes lógicamente
- No interconectan diferentes arquitecturas de Enlace de Datos
- Utilizan el proceso de aprendizaje de la capa MAC, proceso de envío y proceso de filtración

- No alteran las tramas
- Son independientes de las capas superiores
- Tráfico de envíos de *multicast* y *broadcast*

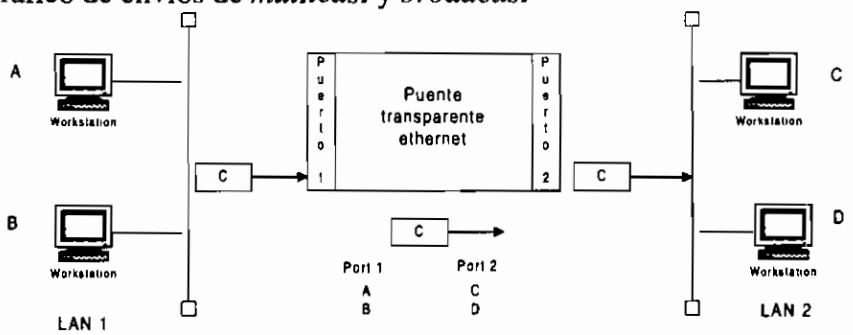


***Figura 3.10* Puente transparente Ethernet**

C.2 Puentes de árbol de cruce transparente

Como las redes crecen y comienzan a ser más complejas, la posibilidad de crear múltiples caminos o lazos entre las LANs se incrementa. Los lazos pueden causar estragos a una red basada solamente sobre puenteo transparente. La duplicación de paquetes y *broadcast*, degradarán el rendimiento de la red.

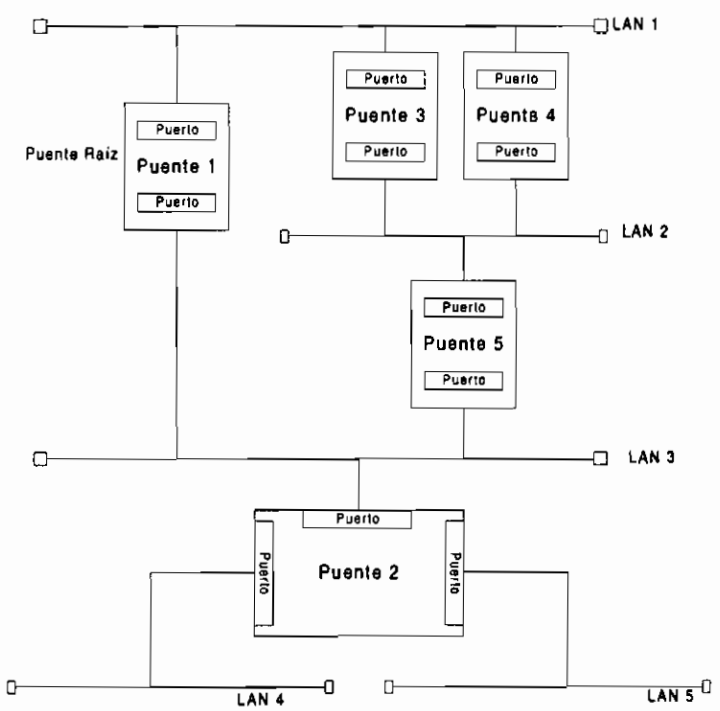


***Figura 3.11* Puentes de árbol de cruce transparentes**

Para combatir el problema de lazo activo se desarrolló un algoritmo de puenteo conocido como *Spanning tree Algorithm (STA)*. El algoritmo STA provee la siguiente funcionabilidad:

- Configura una topología activa predecible de LANs puenteadas dentro de un único árbol de puentes tal que haya al menos un camino lógico entre cualesquiera dos segmentos de LAN; eliminando así cualquier posibilidad de lazos en la red.
- Provee un camino tolerante a fallas utilizando reconfiguración automática de la topología del árbol de puentes como un resultado de falla en un puente o por desperfecto en el camino de datos.
- Consume una cantidad mínima de ancho de banda para establecer y mantener un camino del árbol de puentes.
- Su operación es transparente a los nodos finales

La creación del árbol de puentes comienza con el establecimiento de un puente raíz en una LAN puenteada.

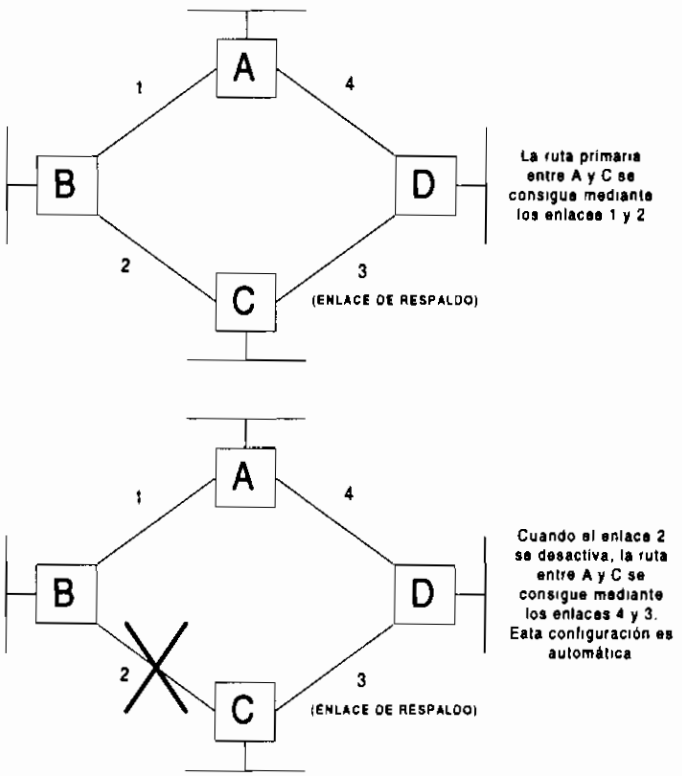


***Figura 3.12* Reconfiguración de caminos ante una falla de enlace**

La creación de un árbol de puentes dentro de una LAN puenteada se resume en las siguientes funciones:

- El puente con el identificador de puente de valor más bajo (configurado en el puente o calculado desde una dirección de la capa MAC del puente) podría ser el puente raíz.

- Los puentes envían unidades de datos *(Bridge Protocol Data Units - BPDUs)* a cada uno de los otros puentes para comunicarse y calcular el costo de camino al puente raíz.
- El pórtico designado para cada LAN es el pórtico del puente para el cual el valor del costo de camino al puente raíz es el más bajo.
- Si dos o más pórticos del puente tienen el mismo valor del costo de camino a la raíz, los identificadores del puerto son usados como *tie breakers* (seguros de enganche).

La reconfiguración del árbol de puentes (figura 3.12) comienza cuando un puente no recibe BTDUs desde sus vecinos. Una vez que un puente no ha recibido más BTDUs aquel tampoco tiene un camino de retorno al puente raíz. Los puentes esperan hasta la expiración de un temporizador *(Maximum-Age timer)* para que ellos comiencen a elegir el proceso en el que todos los puentes determinan cual de los puentes restantes comenzará a ser el nuevo puente designado. Todos los pórticos del puente son bloqueados y pasan al estado de aprendizaje, donde los BPDUs son enviados y recibidos pero el tráfico de la estación no pasa.

Después de que el temporizador presente ha expirado, los pórticos designados sobre un puente son localizados dentro del proceso de aprendizaje. Luego que el temporizador de espera de envío ha expirado, el pórtico del puente designado cambia del estado de bloqueado a estado de envío, y los BPDUs son enviados para actualizar el puente raíz de la nueva configuración. El algoritmo STA permite una topología de red dinámica y garantiza una topología libre de lazos.

C.3 Puente de enrutamiento de fuente

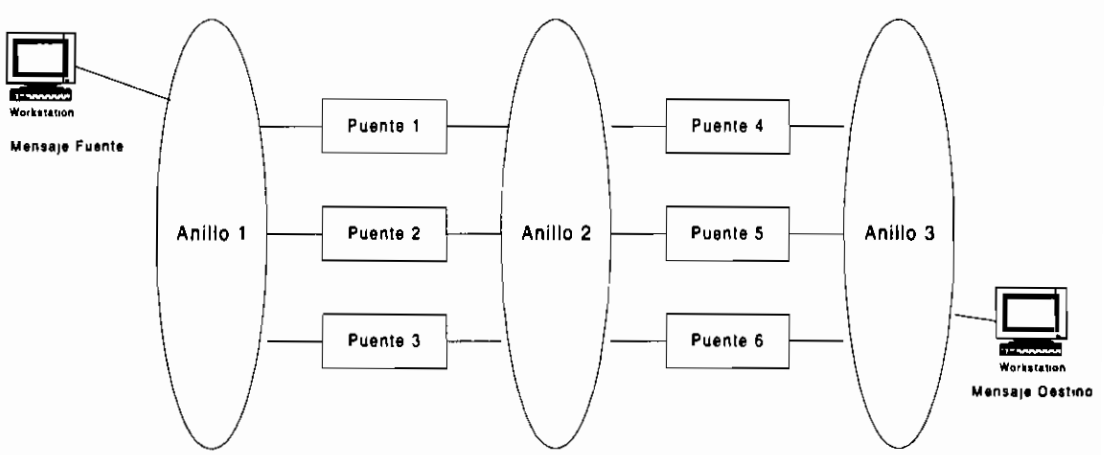


***Figura 3.13** Puentes de enrutamiento de fuente (source-routing)*

El término enrutamiento de fuente (*source-routing*) fue utilizado por IBM para describir un método de puentear tramas a través de redes *Token-Ring*. El enrutamiento de fuente requiere que el mensaje fuente proporcione la información necesaria para entregar un mensaje a su recipiente; de esta manera el mensaje fuente es responsable de determinar la dirección de su destino. La

información del enrutamiento de fuente consiste de una lista de números de anillos y puentes que determina la ruta al destino del mensaje. Desde que el mensaje fuente requiere especificar la ruta al destino del mensaje, un proceso de descubrimiento de ruta es requerido.

La información del enrutamiento de fuente es recopilada y depositada dentro de un RIF (*Routing Information Field*) de la trama IEEE 802.5.

El RIF es incluido si la trama deja la LAN *Token-Ring*, debiendo en este caso incluirse los siguientes campos:

- **Control de ruta-** (2 bytes) son indicadores de *broadcast*, longitud del RIF, bit de dirección, bit de trama más grande, bits reservados.
- **Designador de ruta-** (2 bytes) identifica los campos del designador de ruta que definen el camino formal. Este campo incluye el número del anillo (12 bits) y el número de puente (4 bits) de cada LAN que atraviesa.

Algoritmo de Enrutamiento de Fuente Token-Ring

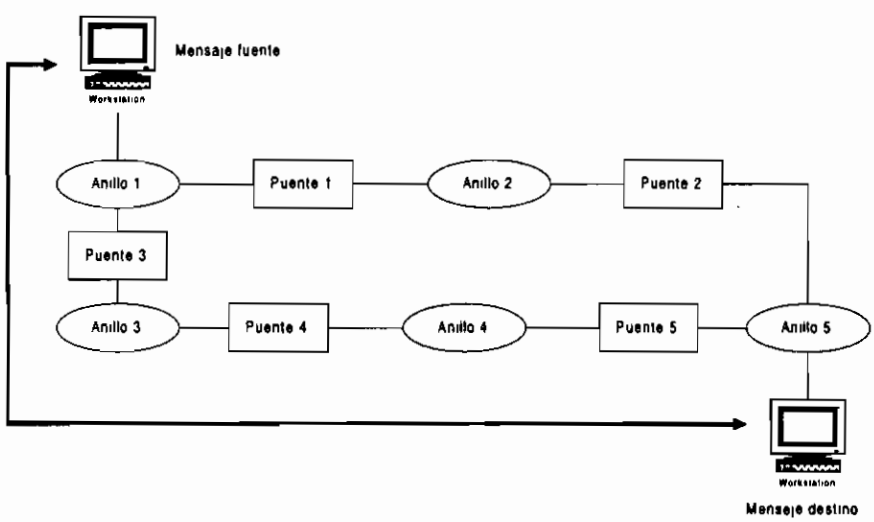


Figura 3.14 Transmisión de paquetes a través de puentes que utilizan el algoritmo de fuente

La estación fuente debe determinar la ruta que debe tomar hasta la estación destino. Para descubrir esta ruta, la siguiente secuencia de eventos ocurre:

1. La estación fuente emite un único paquete explorador de ruta que es enviado a través de la topología de multi-anillo entera.
2. El destino responde a los paquetes descubiertos con un Explorador de Todas las Rutas (*All Routes Explorer*).
3. Todos los puentes propagan la trama *All Routes Explorer*. Cuando un puente recibe una trama para enviar a un anillo, el puente envía la trama al anillo y añade su propio número de puente. El número del

anillo enviador es añadido al campo RIF de la trama en el campo del Designador de Ruta.

4. El mensaje fuente almacena la información RIF de la primera respuesta que recibe y la utiliza en todas las otras tramas al destino. El campo RIF permite hasta 7 ó 14 saltos a través de puentes.

La mayoría de las LANs *Token-Ring* son limitadas hasta una cuenta máxima de 7 saltos. El programa de puenteo IBM es capaz de implementar el IBM STA a lo largo de un SRB (*Single Route Broadcasting*) de modo automático para proveer redundancia dinámica así como minimizar el tráfico de *broadcast*.

C.4 Puentes de enrutamiento de fuente transparente

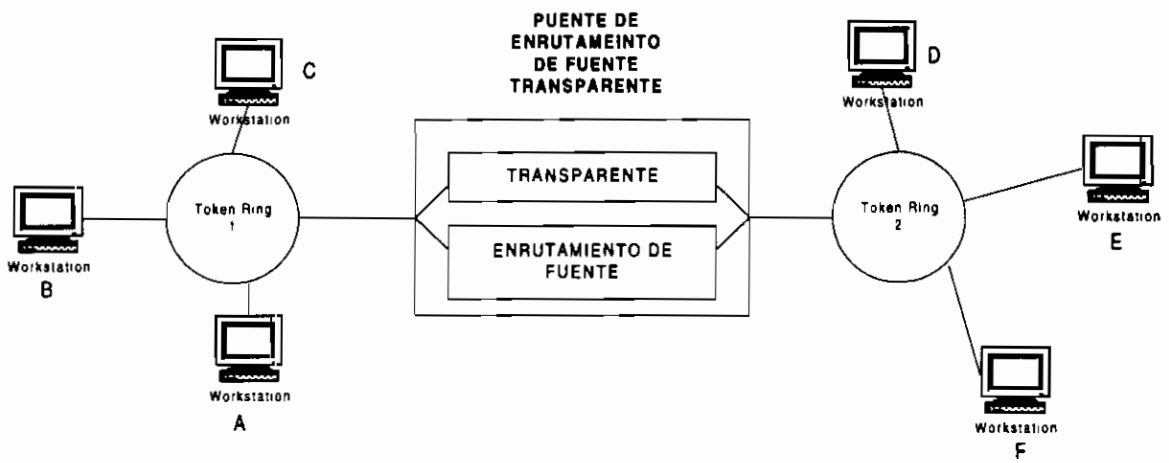


***Figura 3.15** Puente de enrutamiento de fuente transparente*

En medios de red típicos, se requieren paquetes con soporte para puentes transparentes y puentes de enrutamiento de fuente.

Un puente con enrutamiento de fuente transparente es una combinación de un puente de enrutamiento de fuente con un puente transparente, que provee una conexión de redes entre LANs que tienen arquitecturas de enlace de datos de enrutamiento de fuente y no enrutamiento de fuente. Con un puente SRT (*Source Route Transparent*), los sistemas de redes pueden interconectar y correr diferentes tipos de protocolos simultáneamente, incluyendo paquetes con enrutamiento y no enrutamiento de fuente.

En la figura 3.15, los PCs A y F están corriendo *software* de LAN que requiere información de enrutamiento de fuente para enviar paquetes entre ellos (ejemplo: ellos están usando una aplicación que utiliza *Netbios*). Los PCs B, C, D y E están corriendo *software* de no enrutamiento de fuente. El puente SRT utilizará el modo de puenteo transparente cuando maneje tramas de no enrutamiento de fuente, y utilizará modo de enrutamiento transparente cuando utilice tramas de enrutamiento de fuente.

Las principales características de puentes SRT son:

- Usados para conexiones de locales o remotas LAN-LAN
- No separan lógicamente a las redes
- Soportan tanto puenteo de enrutamiento de ruta como transparente
- Utiliza el algoritmo estándar de enrutamiento de ruta
- Es susceptible al tráfico *multicast* y *broadcast*

C.5 Encapsulamiento

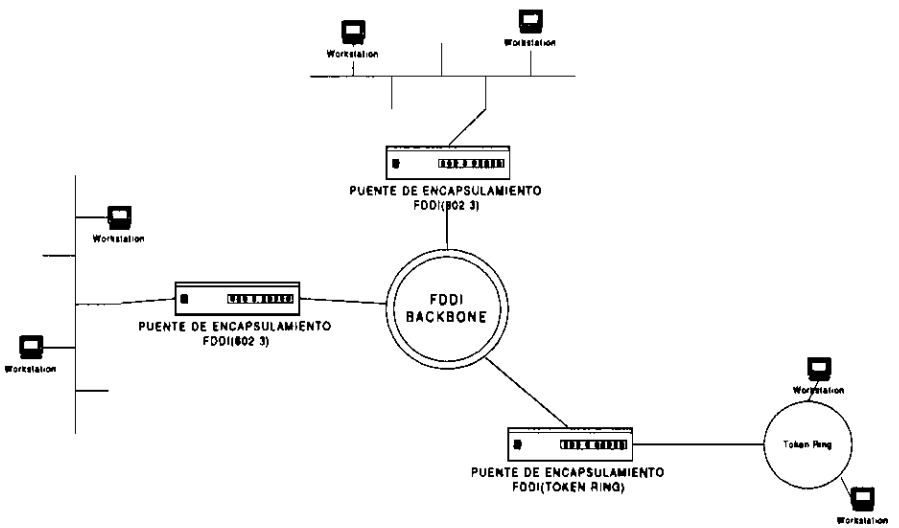


Figura 3.16 Puentes de encapsulamiento

Un puente de encapsulamiento provee servicios de conexión de LAN por encapsulamiento total de la trama original dentro de una nueva envoltura asociada con otro tipo de LAN. Un puente de encapsulamiento es generalmente asociado con topología *backbone* tales como conexiones IEEE 802.3 y 802.5 a FDDI. Los puentes de encapsulamiento tienen las siguientes características:

- Utilizado para conexiones locales y remotas LAN-LAN
- Conecta LANs del mismo o diferente medio físico
- Encapsula la capa de enlace de datos de una LAN dentro de la capa de enlace de datos de la otra
- No altera la trama desde el nodo fuente al nodo destino en ninguna parte del camino
- Es propietario del vendedor
- Añade cabecera a la trama de transmisión
- Es suceptible al tráfico de *multicast* y *broadcast*
- No separa lógicamente a las redes
- No permite comunicación entre diferentes tipos de LANs

El procesamiento realizado por un puente de encapsulamiento es dependiente de las arquitecturas de enlaces de datos que están presentes. No se procede a quitar cabeceras de protocolo. La integridad de las tramas originales IEEE 802.3 y 802.5 o FDDI es mantenida con un puente de encapsulamiento.

C.6 Translacional

Un puente translacional es una forma especial de un puente transparente que permite una conexión de red entre LANs que tienen diferentes arquitecturas de las capas de enlace de datos y física (ej. *Ethernet* y *Token-Ring*). Los puentes translacionales tienen las siguientes características:

- Se utilizan para conexiones locales LAN-LAN
- No separan las redes lógicamente
- Traslada desde un tipo de capa de enlace de datos a otra
- Es independiente del protocolo de la capa de red, pero depende de la capa de enlace de datos
- Es susceptible al tráfico de *multicast* y *broadcast*

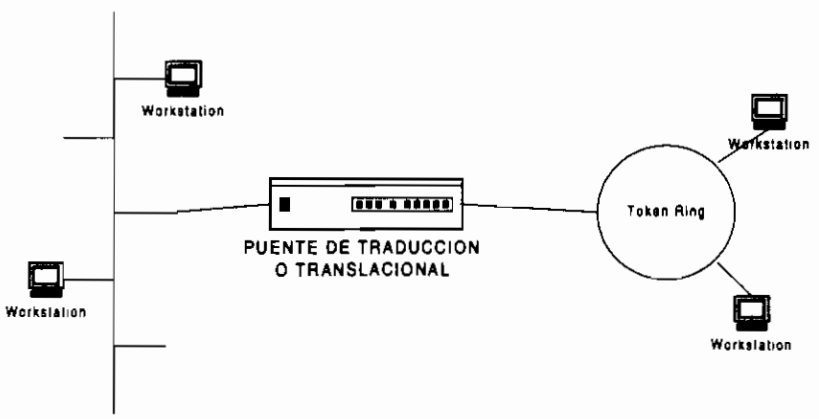


***Figura 3.17** Conexión entre una red Ethernet y una Token-Ring utilizando un puente de traducción*

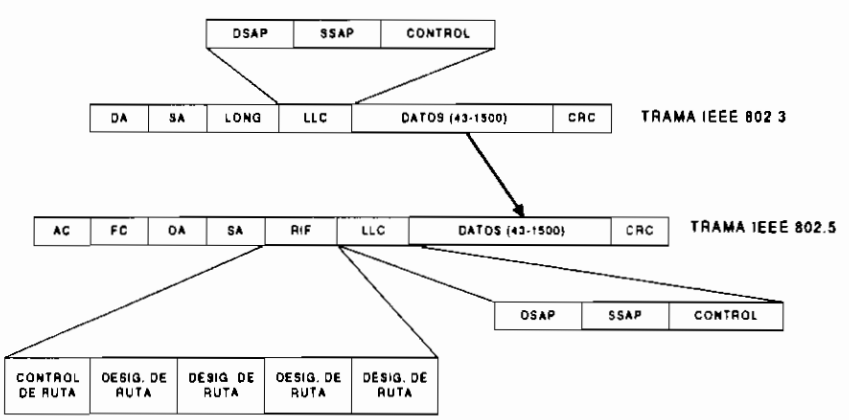


***Figura 3.18** Tramas IEEE 802.3 y 802.5*

Un puente translacional provee servicios de conexión por manipulación de la envoltura de la trama asociada con cada tipo de LAN. El procesamiento realizado por un puente translacional es relativamente directo, porque las envolturas *Ethernet*, *Token-Ring* y FDDI son similares.

Debido a que cada arquitectura de LAN tiene diferentes tamaños de trama, cada LAN debe ser configurada para transmitir la trama que tenga el tamaño de mínimo común denominador de todos los segmentos dados, para que los protocolos de la capa de enlace de datos no permitan la fragmentación de mensajes.

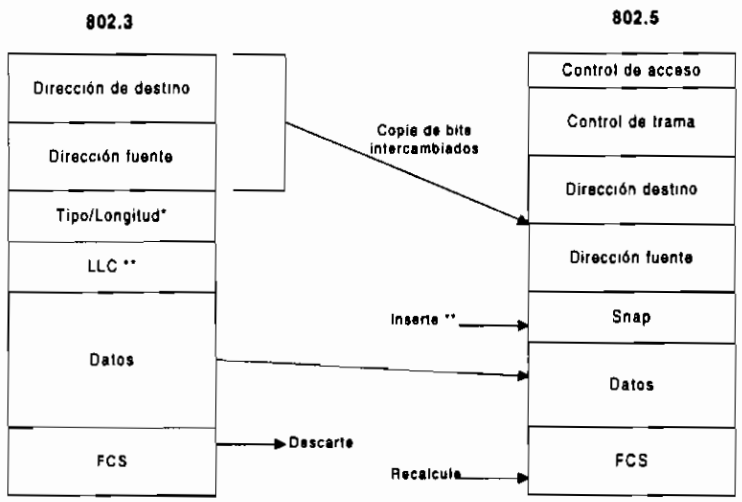


***Figura 3.19* Disposición de tramas IEEE 802.3 y 802.5**

Puesto que el formato de las direcciones MAC sobre IEEE 802.3, IEEE 802.5 y FDDI son diferentes, los puentes translacionales deben acomodar estas diferencias.

Las redes *Ethernet* utilizan un orden de bits canónico lo cual simplemente significa dentro de su propia trama, el bit menos significativo es siempre transmitido primero. FDDI y *Token-Ring* utilizan orden de bit no canónicos, es decir que el bit más significativo de un byte es el primero que se transmite. Así, un puente translacional que traduce tramas entre *Ethernet* y *Token-Ring* o *Ethernet* y FDDI, debe manejar el reordenamiento de las direcciones de fuente y destino de cada trama enviada entre estas redes. También, se debe notar que para las tramas *Ethernet* V2.0, una cabecera SNAP debe ser insertada para un formato de trama FDDI.

3.2.2.4 *Switches* (conmutadores)

A. Introducción a los conmutadores y sus aplicaciones

A.1 ¿Por qué son necesarios en las LAN?

Los conmutadores pueden manejar el incremento del tráfico y cuellos de botella que son resultado del crecimiento de las redes en los últimos años. Los conmutadores proveen soluciones de alto rendimiento proporcionanado anchos

de banda dedicados y salidas con grandes capacidades de transmisión de paquetes a usuarios y servidores con un bajo costo por puerto. También proveen conexiones de red de altas velocidades, permitiendo mantener la infraestructura de red existente.

A.2 ¿Qué es un conmutador?

Los conmutadores de LAN son dispositivos que han evolucionado como un intento de resolver algunos de los problemas existentes encontrados en otros dispositivos, tales como puentes y ruteadores. El tiempo de latencia es considerado como el tiempo transcurrido desde que una trama es recibida en un pórtico del conmutador hasta que la trama sale por el pórtico que la llevará a su destino. Los conmutadores son mucho más rápidos que los puentes multipuerto. Sin embargo, debe considerarse que los conmutadores no son arquitectónicamente rápidos, pues ellos no son construidos por velocidad, pero ellos son funcionalmente rápidos. Su funcionabilidad es la clave de su acogida, ya que una de sus metas es mover un paquete tan rápido como sea posible a su destino específico con el menor número de decisiones posibles. Los conmutadores mueven los paquetes tan rápido, que parecen estar procesando conversaciones en paralelo, combinando las redes relativamente más lentas conectadas a ellos dentro de un *backbone* de alta capacidad y baja latencia[25].

A.3 ¿Qué provee un conmutador?

Algunos de los beneficios comunes son: incremento de la capacidad, segmentación, conversaciones paralelas, y conectividad para LANs. Además, debido a que los conmutadores son típicamente implementados en la capa 2 del modelo de referencia OSI, ellos son dispositivos más simples y fáciles de utilizar que los ruteadores.

Las aplicaciones comunes de un conmutador LAN incluyen:

- Segmentación y aislamiento de la red de estaciones de alto tráfico, tales como servidores.
- Creación de redes virtuales y/o dominios *broadcast*.
- Creación de un *backbone* de red colapsado.
- Alta salida para estaciones de alto rendimiento.

A.4 Segmentación

Un segmento está definido como un grupo de nodos que comparten el mismo dominio de colisión. Los *switches* o conmutadores son muy utilizados para enlazar puentes y separar dominios de colisión. La meta es incrementar la salida a cada usuario decrementando el número de estaciones que deben estar contenidas en un ancho de banda compartido. El conmutador separa los dominios de colisión, tal como un puente. Esto también mantiene una matriz de direcciones destino y pórticos físicos asociados con la dirección, así que aquel

[25] En lugar de "tiempo de latencia" se utiliza también "latencia"

puede conmutar tramas. Una trama de llegada es solamente transmitida sobre el pórtico asociado con la dirección de destino de la trama. El número de la dirección de destino soportado por cada pórtico es dependiente del modelo y proveedor del conmutador, pero puede estar en el rango de uno a mil.

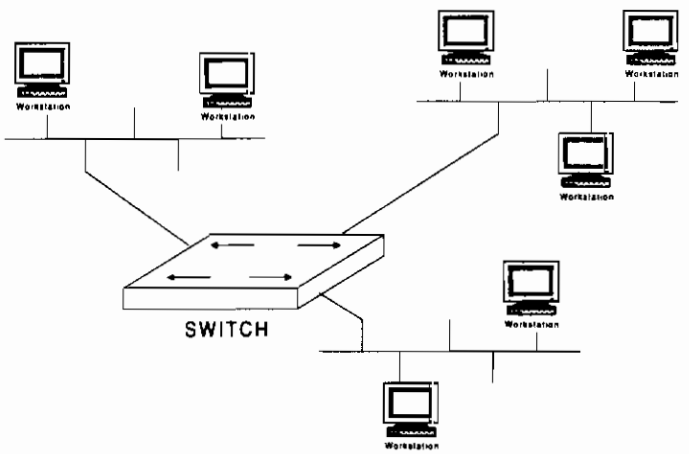


***Figura 3.20** Utilización de switches para segmentar redes y dominios de colisión*

Algunas aplicaciones, tales como multimedia, no pueden tolerar grandes demoras o grandes cantidades de *jitter* (variaciones en la demora).

A.5 Microsegmentación

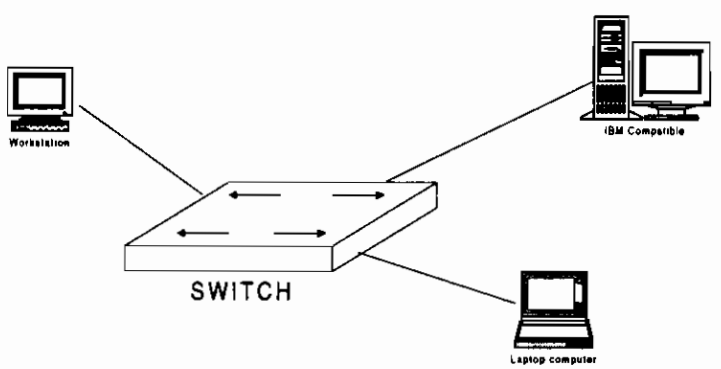


***Figura 3.21** Microsegmentación definida en un switch (una estación por pórtico)*

Si se decrementa el número de estaciones en las que deben estar contenidas para compartir el ancho de banda, la situación más deseable es tener una estación por pórtico del conmutador. La estación no tiene que competir por ancho de banda con otras estaciones. Si el conmutador entero es microsegmentado (todos los pórticos tienen solamente una estación por segmento), cualquier estación parecerá tener una conexión dedicada a cualquier otra estación en el total del ancho de banda del medio de conexión. Típicamente, la microsegmentación es empleada en estaciones de alta utilización, tales como servidores de archivos, *gateways* de correo electrónico y servidores de impresión. En casos de utilización muy pesada, se pueden utilizar múltiples adaptadores de red

instalados en la misma estación, haciendo que cada adaptador se conecte con un pórtico diferente del conmutador.

El conmutador puede servir como una interfaz de alta salida (*throughput*) entre múltiples servidores y grupos de usuarios; múltiples conmutadores pueden conectarse juntos para formar un *backbone* de alta capacidad vía *full duplex* y *port trunking*.

La característica *full duplex*, dobla la capacidad de conexión entre dos dispositivos, mientras que *port trunking* permite que algunos puertos puedan ser conectados juntos y tratados como un único puerto de alta velocidad.

Dominios de *Broadcast* y LAN virtuales

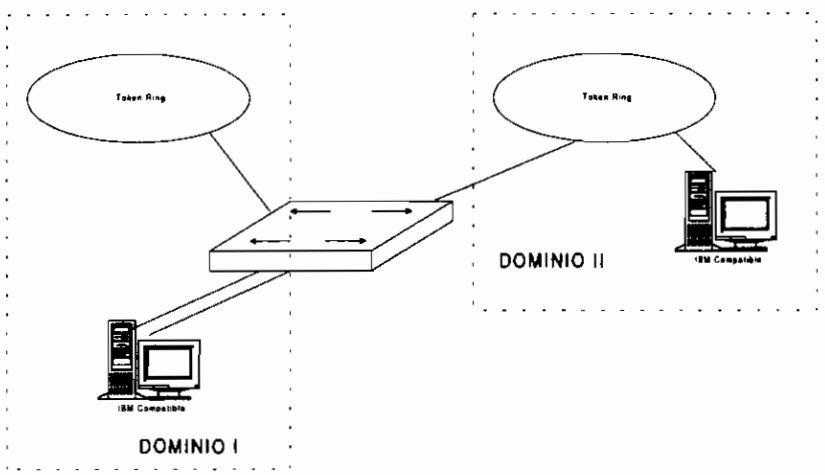


***Figura 3.22** Separación de dominios de broadcast utilizando switches*

Debido a que un conmutador intenta mantener una topología de red lo más plana posible (todas las estaciones se ven con las otras como si estuvieran en la misma red), las tramas de *broadcast* y *multicast* deben ser enviadas a todos los pórticos de salida conectados al conmutador. En algunos casos, esto crea tráfico de red innecesario. Para controlar este tráfico de *broadcast* orientado, los administradores pueden agrupar pórticos, creando una red virtual. Este grupo de pórticos es llamado un dominio de *broadcast*. Si la trama que llega al conmutador está determinada a ser una trama de *broadcast* o *multicast*, esa trama es transmitida sólo a los pórticos del dominio correspondiente a su red virtual, evitando de esta manera que toda la red se inunde con tráfico *broadcast o multicast* innecesario para los otros dominios.

A.6 *Backbone* colapsado

Se llama *backbone* colapsado al *backbone* que tiene una topología física radial o estrella, y tiene como punto de concentración de la estrella un dispositivo de conectividad (generalmente conmutadores o ruteadores). Se utiliza el término colapsado para indicar que todos los segmentos del backbone "colapsan" hacia el dispositivo de conectividad central.

Los conmutadores permiten separar segmentos LAN para interconectarlos unos con otros. Es importante que el centro del *backbone* colapsado sea un dispositivo con capacidad de manejar ampliamente el ancho de banda (para permitir altas velocidades), cualidad que los conmutadores tienen en abundancia.

B. Técnicas de conmutación

Operación *half duplex/full duplex*

Las tecnologías de LAN son normalmente operaciones *half duplex*. Esto significa que un adaptador de red puede ser transmitir o recibir datos en cualquier momento, pero no puede realizar ambas operaciones simultáneamente. Algunos proveedores de conmutadores han implementado adaptadores *full duplex*, permitiendo que las estaciones se conecten directamente al conmutador para transmitir y recibir datos de los conmutadores simultáneamente. Esto permite velocidades de transmisión mucho más altas entre adaptadores y conmutadores. La aplicación típica para estos adaptadores son servidores de archivo/correo/impresión los cuales deben manejar altos volúmenes de tráfico. No hay estándares definidos para operación *full duplex*, así que los adaptadores deben ser adquiridos del mismo proveedor del conmutador.

C. Tipos de conmutadores *Ethernet*

C.1 Corte directo (*cut through*)

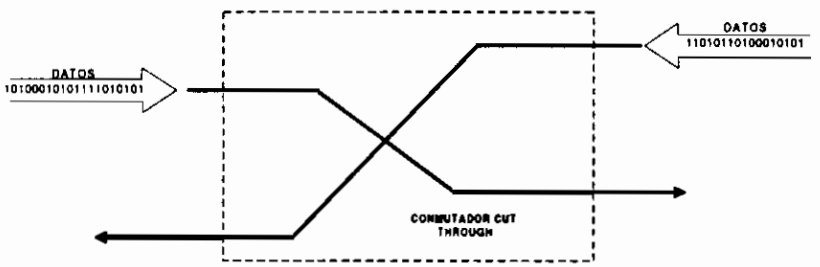


***Figura 3.23** Diagrama de funcionamiento de un conmutador de corte directo (cut through)*

El conmutador *Ethernet* de corte directo consigue muy baja latencia por medio de una conexión entre los puertos entrantes y salientes de conexión. Tan pronto como la cabecera de trama ha llegado sobre el pórtico entrante, ésta es procesada por el conmutador. Para procesar la información de la cabecera, el conmutador verifica la dirección de destino en una tabla de direcciones MAC aprendidas. El conmutador utiliza esta tabla para determinar cual pórtico de salida debería recibir la trama. La trama es entonces enviada al pórtico de salida, usualmente mientras la trama está todavía siendo recibida en el pórtico entrante. La excepción podría ser si el pórtico de salida tiene tramas almacenadas en *buffers* esperando a ser transmitidas o que el medio esté en uso por otra estación. En este caso, el conmutador almacena las tramas en los *buffers* y los transmitirá cuando sea posible.

Los conmutadores de corte directo típicamente no realizan verificación de errores sobre la trama que llega, siempre y cuando la dirección de destino en la cabecera empareje con una de las direcciones de la tabla del conmutador. Si la dirección de destino no es reconocida (no empareja), el conmutador almacenará las tramas en *buffers* y verificará el FCS (*Frame Check Sequence*- Secuencia de verificación de la trama) para validar la trama. Si la trama es buena, el conmutador enviará la trama a todos los pórticos de salida. Si la trama es mala, será descartada. Esta técnica previene errores de cabecera provenientes de transmisiones falsas.

C.2 Almacene y envíe (*Store and forward*)

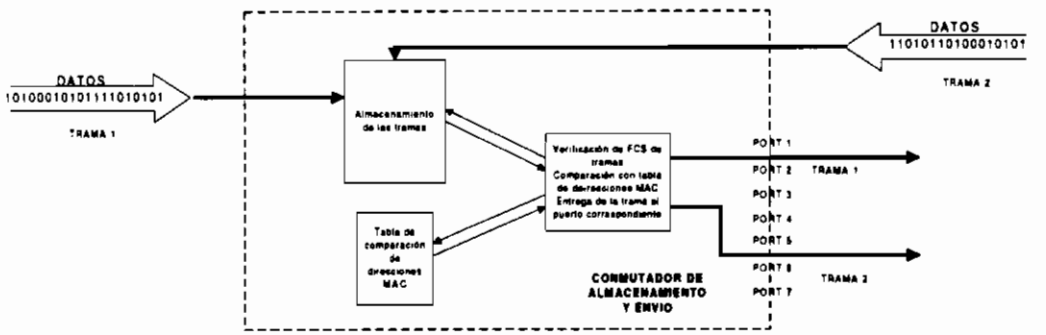


***Figura 3.24** Diagrama de funcionamiento de un conmutador de almacenamiento y envío*

Un conmutador *Ethernet store and forward* opera muy parecido a un puente multipuerto. Cada trama entrante es almacenada completamente y el FCS es validado antes de que la cabecera de la trama sea procesada y transmitida sobre el pórtico de salida. Para procesar la información de la cabecera, el conmutador verifica la dirección de destino contra una tabla de direcciones MAC aprendidas. El conmutador usa esta tabla para determinar cual pórtico de salida debería recibir la trama. La trama es entonces transmitida sobre el pórtico saliente, a menos que este pórtico tenga tramas esperando a ser transmitidas o el medio esté en uso por otra estación. En estos casos, el conmutador almacena la trama en el pórtico de salida y lo transmitirá cuando sea posible.

El almacenar la trama antes del procesamiento y transmisión, permite que los conmutadores de almacenamiento y envío puedan proveer características extendidas. Debido a que el FCS es calculado para todas las tramas, el conmutador puede eliminar transmisión de tramas corruptas. Algunos proveedores de conmutadores de almacenamiento y envío también proveen subred virtual adicional y servicios de dominios *broadcast* por verificación de la información de la capa de red en la trama almacenada. Además pueden estar disponibles capacidades de filtraje de trama (versus la información basada en la capa de red).

D. Tipos de conmutadores *Token-Ring*

D.1 Corte directo (*Cut through*)

La conmutación de corte directa *Token-Ring* trabaja similar a la conmutación de corte directa *Ethernet*. La conexión entre los pórticos de entrada y salida es realizada tan pronto como la información de la cabecera de la trama ha sido leída y procesada. La dirección de destino de la trama es verificada en la tabla del conmutador de las direcciones MAC para determinar cual pórtico saliente puede ser utilizado. El pórtico saliente entonces usa los servicios de prioridad *Token-Ring* para solicitar el token (testigo) y comenzar a transmitir la trama. La trama entrante es completamente almacenada solamente si hay otras tramas esperando ser transmitidas sobre el pórtico saliente. El pórtico saliente puede no reclamar el testigo, debido al tráfico desde las estaciones de más alta prioridad, debido a que la trama que está siendo conmutada entre anillos de 4 y 16 Mbps, o si el anillo conectado al pórtico saliente está en *beaconing*[26].

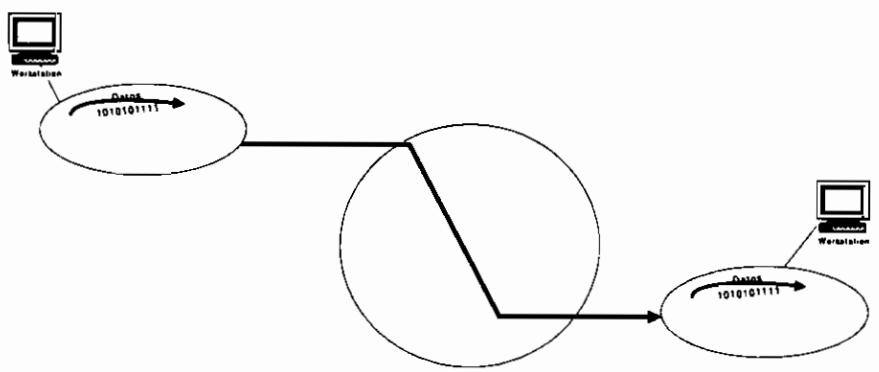


***Figura 3.25** Conmutador cut through para redes Token-Ring*

D.2 Fuente-Ruta (Source-Route)

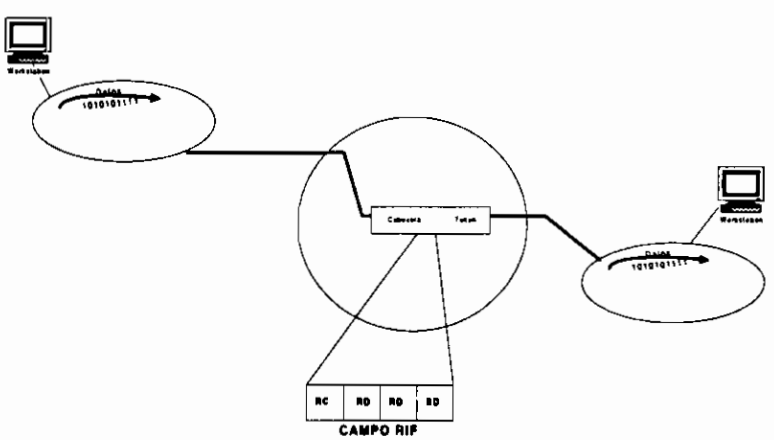


***Figura 3.26** Diagrama de funcionamiento de un conmutador Token-Ring*

[26] *Beaconing* es una condición de error en redes *Token-Ring*.

Los conmutadores *Token-Ring* operan sobre los mismos principios generales de un puente fuente-ruta. El conmutador busca información en el RIF (*Route Information Field*) para indicar cual pórtico de salida puede ser usado. El conmutador entonces transmitirá la trama al pórtico de salida tan pronto como pueda reclamar el testigo para ese anillo. Si el RIF indica un *broadcast* a todas las rutas, el conmutador copiará la trama a todos los pórticos de salida que tengan una única ruta de *broadcasting* habilitada. Si el campo RIF no está presente, la trama es descartada. Esto, en efecto, requiere fuente-ruteo sobre todas las estaciones si la red está microsegmentada.

E. Conmutación de medios LAN mezclados

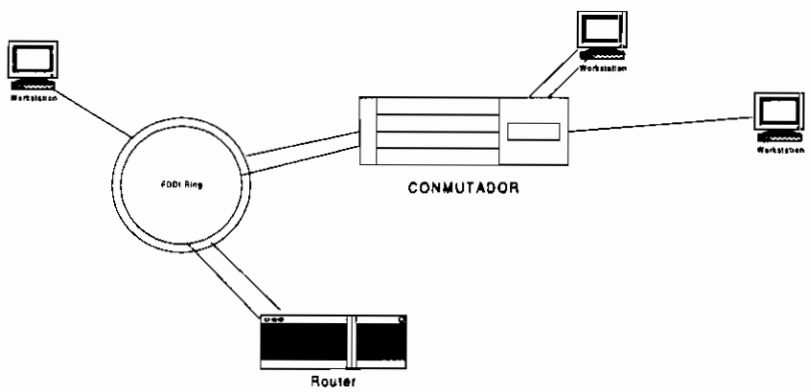


***Figura 3.27** Conmutadores para medios LAN mezclados*

Estos conmutadores contienen pórticos *Ethernet* o *Token-Ring* para acceso departamental o de grupos de trabajo (o para estaciones directamente conectadas). Ellos también pueden contener otro tipo de interfaz, usualmente FDDI o ATM para conectarse a un *backbone*. Las tramas son conmutadas entre los puertos *Ethernet* y *Token-Ring*. Las tramas que requieren acceso al *backbone* son puenteadas sobre la red *backbone* utilizando una tecnología de translación de puente en el caso de FDDI. En el caso de ATM, el conmutador actúa como la interfaz ATM para cada dispositivo sobre los pórticos de conmutación, haciendo aparecer al resto de la red ATM que cada dispositivo tiene una interfaz ATM (aunque sea una interfaz de bajo ancho de banda).

Integración de conmutadores

Los conmutadores LAN pueden ser integrados dentro de la red en una variedad de configuraciones, cada una con su propio grupo de beneficios. Es importante que al integrar conmutadores, se considere lo siguiente: topología de red, costo del equipo y recursos de personal (que resolverán los problemas de conmutación), y cómo los cambios en la topología de la red afectarán el futuro de la red. Los conmutadores pueden integrarse dentro de una variedad de topologías de red existentes como sigue:

- Conmutadores reemplazando los repetidores (*hubs*) en una red plana
- Conmutadores añadidos a una red puenteada

- Conmutadores añadidos a una red ruteada

a. Redes basadas en *hubs*

Los conmutadores LAN pueden ser usados en conjunto con los *hubs* tradicionales para proveer segmentación de la red, mientras se mantiene una topología plana de una red basada en *hubs*. En este caso, todos los *hubs* departamentales existentes son dejados en su lugar y funcionando. Ahora, cada *hub* tiene su propio dominio de colisión, reduciendo la posibilidad de colisiones. Por otro lado, todos los *hubs* departamentales son reemplazados con *hubs* conmutadores, proveyendo a cada departamento de su propia microsegmentación. Las redes son interconectadas al conmutador-*backbone*, proveyendo un *backbone* colapsado para la interconexión. Si los *hubs* de conmutación departamentales son conectados al conmutador-*backbone* por medio de conexiones *full duplex*, sus salidas al *backbone* son efectivamente dobladas. Los recursos de red compartidos, tales como servidores de archivos, pueden también ser conectados a su propio conmutador departamental por medio de conexiones *full duplex*.

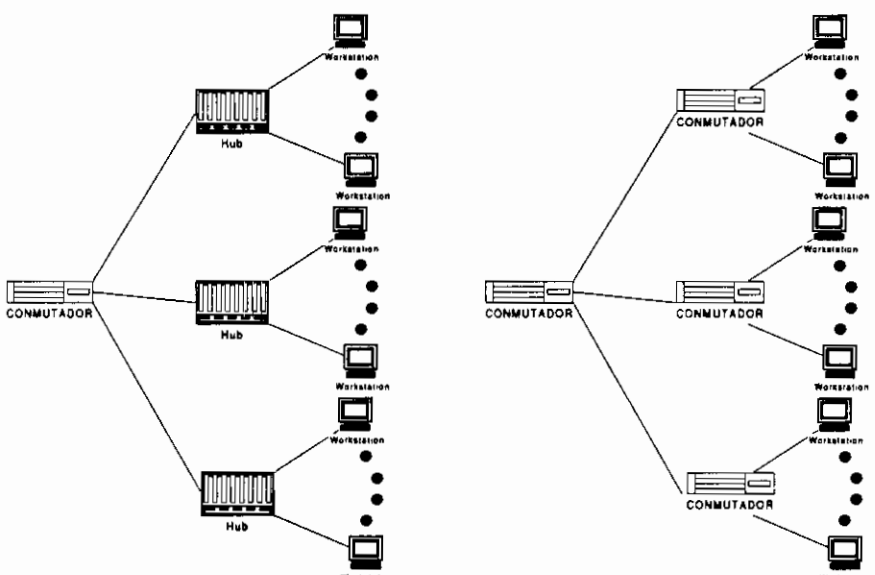


***Figura 3.28** Utilización de conmutadores en lugar de hubs de acceso compartido*

b. Redes puenteadas

Los conmutadores LAN proveen los mismos servicios funcionales como un puente LAN con una latencia mucho más baja. Típicamente los conmutadores son utilizados para reemplazar *hubs* donde la microsegmentación es requerida para usuarios que requieren grandes anchos de banda, dejando el *backbone* puenteado en su lugar (ver figura 3.29). Otra solución podría ser reemplazar *hubs* y puentes en la LAN, dejando únicamente a los puentes en las conexiones de área amplia en su sitio. Esto mejora el rendimiento en cada LAN sin cambiar la conectividad del área amplia del usuario.

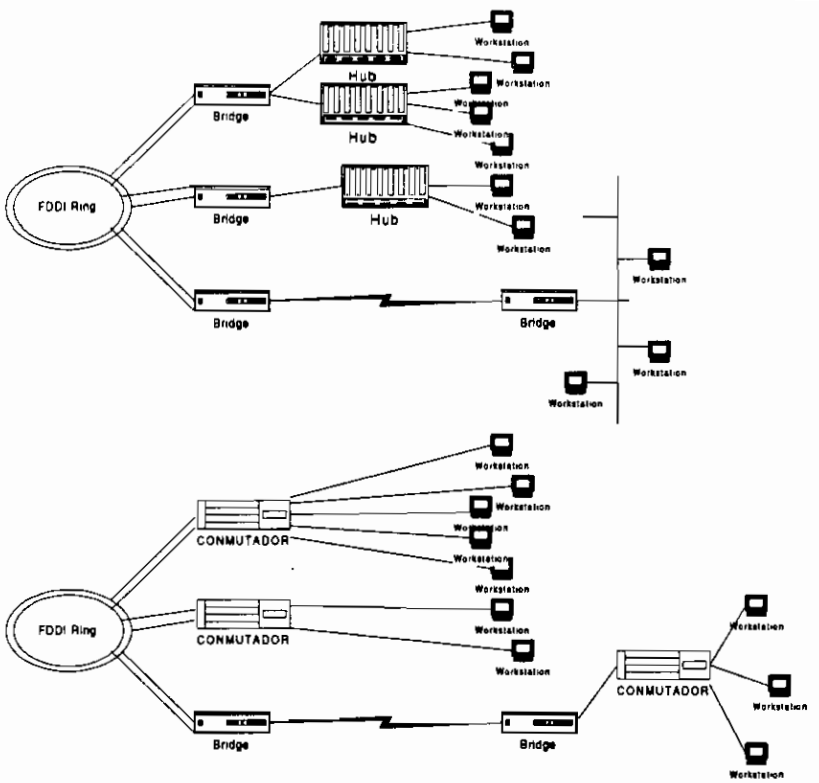


Figura 3.29 Utilización de conmutadores de medios LAN mezclados en lugar de puentes y hubs de acceso compartido

c. Redes ruteadas

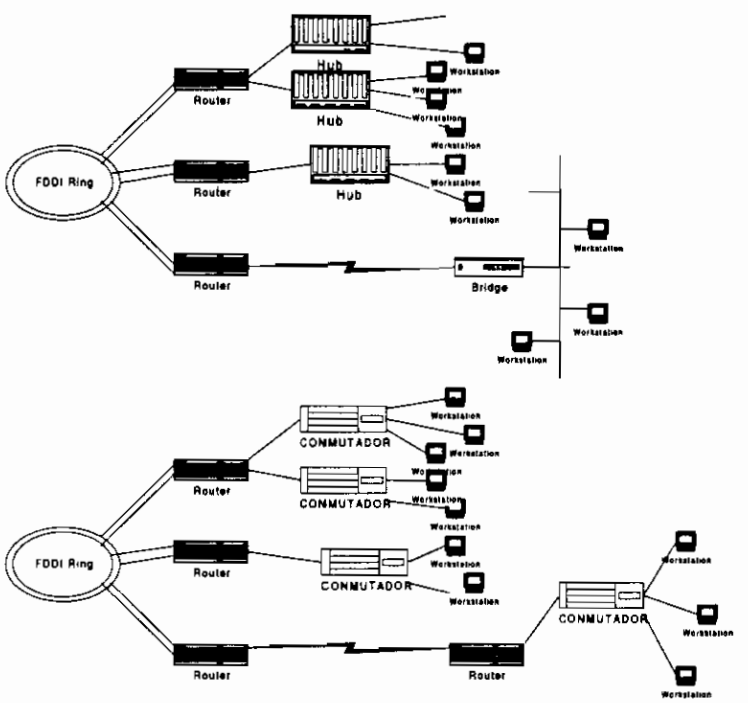


Figura 3.30 Utilización de conmutadores en lugar de hubs de acceso compartido y conectados a ruteadores

Al añadir ruteadores a la internet, se añade complejidad pero se provee mucho mayor control del flujo de datos entre LANs. Además, se proporciona a la red una categoría jerárquica, separando las LANs por direcciones lógicas. Típicamente, los conmutadores son usados para proveer un incremento en rendimiento al ruteador, por segmentación de las estaciones en grupos de trabajo dentro de dominios de colisión más pequeños (ver figura 3.30). El ruteador puede ser conectado a un puerto del conmutador, proveyendo un ancho de banda dedicado al grupo de trabajo. La microsegmentación puede ser usada para asegurar que cada estación tenga su ancho de banda dedicado a todos los otros miembros del grupo de trabajo así como al ruteador.

F. Migración a ATM con conmutadores

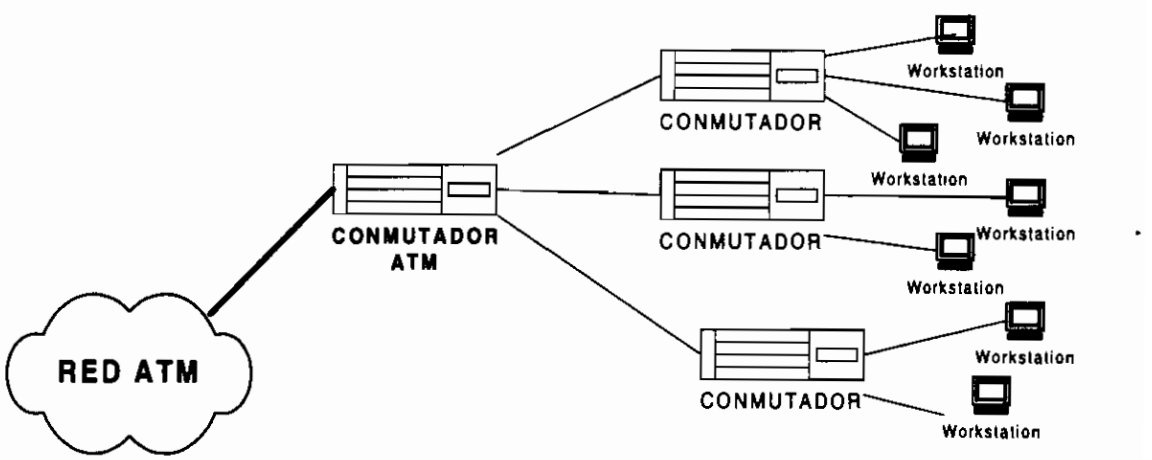


***Figura 3.31** Utilización de conmutadores para conectividad con tecnologías de alta velocidad*

La tecnología de conmutación puede ser usada como un paso transitorio en la migración a tecnología ATM. Los conmutadores con capacidad de soportar ATM pueden ser utilizados para reemplazar *hubs* y/o puentes dentro de la red existente. Esto mejora el rendimiento de grupo de trabajo debido a que se realiza conmutación entre miembros del grupo de trabajo. Esto también provee una forma para que el grupo de trabajo se conecte al *backbone* ATM para acceso conmutado a otros grupos, todavía sin cambiar el cableado original o interfaz. En un momento determinado, el conmutador LAN y los miembros de su grupo de trabajo asociado, podrían ser trasladados a un conmutador ATM con conexiones ATM al escritorio.

3.2.2.5 Ruteadores

Los ruteadores operan en la capa 3 del modelo de referencia OSI. Como los puentes, los ruteadores proveen a los nodos finales comunicación transparente entre dos redes físicamente separadas. A diferencia de los puentes, los ruteadores mantienen las identificaciones lógicas de cada segmento de red en la internet y guardan un rastro de las redes lógicas en una tabla de ruteo.

A. Conmutador versus ruteador

El conmutador es un dispositivo que no intenta reemplazar al ruteador multipuerto. En efecto, en grandes redes los dos son usados juntos para proveer una solución completa. Un conmutador intenta proveer una salida amplia entre grupos de trabajo y servidores con la mínima latencia. El ruteador no intenta proveer una alta salida ni baja latencia. Su propósito incluye:

- Aislar LANs separadas (*Firewalls* de red)
- Proveer decisiones de enrutamiento inteligentes para elegir el mejor camino utilizando algoritmos de estado de enlace o vector de distancia
- Proveer el mejor enlace y redundancia
- Filtración de tráfico basados sobre protocolo (IP, IPX, NFS, SNA, DECnet, etc)
- Conectividad WAN (T1, X.25, etc)

B. Aplicaciones del ruteador

Los siguientes tópicos, cubren la mayoría de los requerimientos de usuario final . para interconectividad con tecnología de enrutamiento: segmentación, arquitecturas de enlace de datos, fragmentación de paquetes, redundancia, enrutamiento alterno y administración de red.

B.1 Segmentación

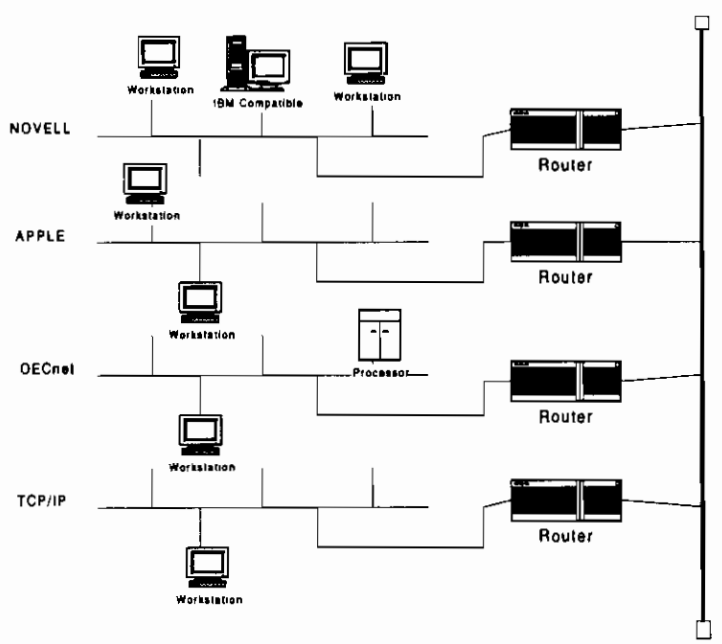


Figura 3.32 Conexión de segmentos utilizando ruteadores

La segmentación de una red significa separarla en alguna subredes más pequeñas. Como los puentes, los ruteadores pueden segmentar LANs basadas en protocolos de la capa de red (ruteable). La segmentación es realizada por muchas razones: rendimiento, seguridad y control. La mejora del rendimiento puede

cumplirse de varias formas, pero solamente la segmentación de la red es implementada para control de tráfico, proveer protección contra grandes *broadcast*, permitir acceso para especificar recursos y asistir en tareas de administración de la red.

Los ruteadores utilizan listas de acceso o filtros para restringir o permitir el acceso a recursos de estaciones o subredes específicas. Estos filtros permiten que los administradores de red definan los límites para cada interfaz conectado al ruteador. Con filtro de protocolo específicos, los ruteadores deben ser capaces de entender cabeceras de red y campos de protocolos de longitud variable.

Con el control y filtraje adicional que es obtenido con ruteadores, los ruteadores pueden acordar ellos mismos con el camino actual que cada paquete debe tomar a través de la red. Semejante a la base de datos de filtraje utilizado por los puentes en la capa MAC, los ruteadores pueden mantener tablas de enrutamiento que indican que hacer con los paquetes especificados.

B.2 Solución a la interconectividad heterogénea

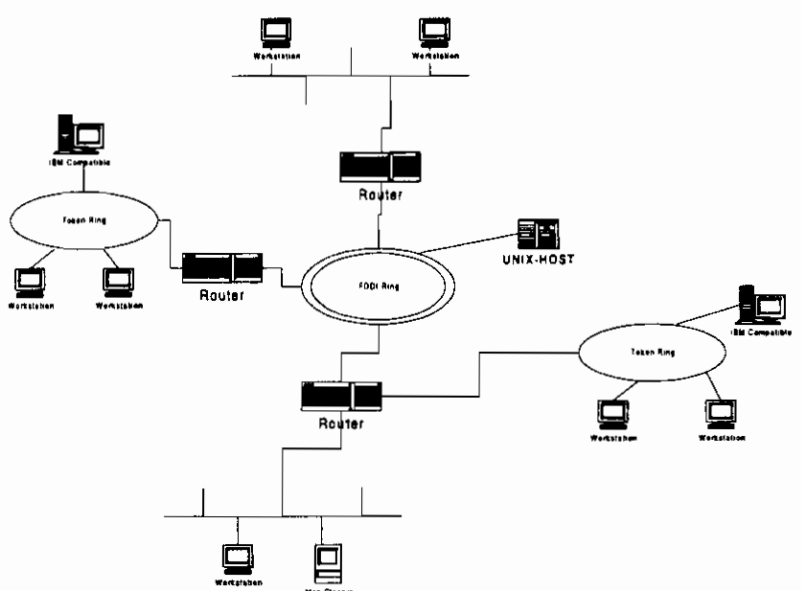


***Figura 3.33** Uso de ruteadores en la interconexión de diferentes tipos de redes*

Pocas redes de empresas grandes son construidas con una única arquitectura de enlace de datos. La mayoría de redes agrupan redes *Token-Ring*, *Ethernet*, *Local talk*. Los ruteadores pueden resolver las diferencias entre arquitecturas mezcladas de la capa de enlace de datos. Estas diferencias son resueltas utilizando técnicas de fragmentación y traslación para varias arquitecturas de enlaces de datos.

3.3 TENDENCIAS TECNOLOGICAS DE ACTUALIDAD Y PROTOCOLOS MÁS COMUNES

Existen muchos *stacks* de protocolos, que tienen relación con cada una de las capas del modelo de referencia OSI. Los protocolos de estos *stacks* pueden estar orientados a funcionar en redes LAN, MAN o WAN.

Nos corresponde el estudio de los protocolos orientados a redes LAN cuya relación con el modelo de referencia OSI sea con las 3 primeras capas: física, enlace de datos y red. Además, en los *stacks* de mayor popularidad se hará referencia a algunos protocolos relacionados con la capa 4: transporte.

Dentro de estos protocolos se hará mención a los siguientes, como los más comunes:

a. Del *stack* de protocolos de Netware
   a.1 MLID
   a.2 LSL
   a.3 IPX
   a.4 RIP
   a.5 NLSP
   a.6 SPX
b. Del *stack* de protocolos TCP/IP
   b.1 IP
   b.2 ICMP
   b.3 RIP
   b.4 OSPF
   b.5 TCP
   b.6 UDP
   b.7 ARP
   b.8 DNS
c. Del *stack* de protocolos DNA
   c.1 *Ethernet* V.2
   c.2 CLNS
   c.3 CONS
   c.4 ISO 8073
   c.5 NSP
d. Del *stack Apple Talk*
   d.1 Local Talk, Ethertalk y Tokentalk
   d.2 AARP
   d.3 DDP
   d.4 RTMP
e. Del *stack* IBM (SNA)
   e.1 *Token-Ring*
   e.2 NCP
   e.3 VTAM
   e.4 APPN
f. Protocolos de la serie IEEE 802.X:

f.1 IEEE 802.2
f.2 IEEE 802.3
f.3 IEEE 802.4
f.4 IEEE 802.5
f.5 IEEE 802.6
f.6 IEEE 802.7
f.7 IEEE 802.8
f.8 IEEE 802.9
f.9 IEEE 802.10
f.10 IEEE 802.11
f.11 IEEE 802.12

Protocolos de alta velocidad

g. FDDI
h. *Fast Ethernet*
i. ATM
j. Gigabit Ethernet

Cada uno de los protocolos mencionados, será descrito en base al tema y la técnica asociados al nivel correspondiente en el modelo OSI.

3.3.1 DEL *STACK* DE PROTOCOLOS NETWARE

El sistema operativo Netware fue creado por Novell, cuya arquitectura de red es centrada en el servidor, a través de la cual los dispositivos de red remotos parecen locales para el usuario.

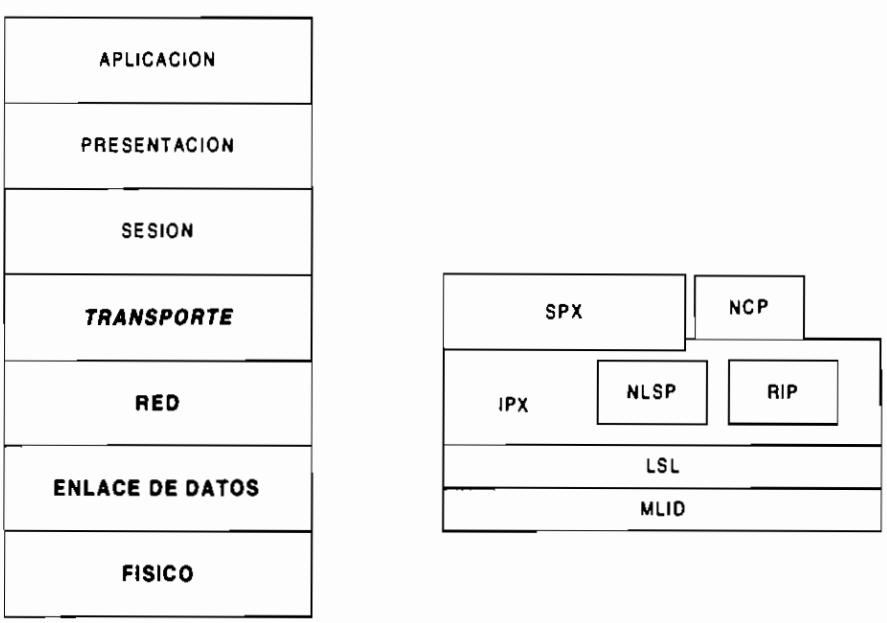


***Figura 3.34** Stack de protocolos IPX/SPX y su relación con el modelo OSI*

Si bien los protocolos pertenecientes al *stack* de protocolos de Netware son modulares y estratificados, los diseñadores de su arquitectura se centraron en suministrar un alto nivel de funcionabilidad sin una adhesión a ningún modelo existente. Por esta razón, los protocolos pertenecientes a este *stack* no encajan plenamente en los siete niveles del modelo de referencia OSI. A pesar de esto, es importante establecer una relación entre los protocolos más reelevantes de este *stack* correspondientes a los cuatro primeros niveles del modelo OSI.

Protocolo	**Nivel OSI**	**Temas**	**Técnicas**
MLID-Controlador de interfaz de enlace múltiple	Enlace de datos MAC	Acceso a medios	Contención* Entrega de testigo* Sondeo* (*asigna cabeceras MAC basándose en el nivel físico)
LSL-Nivel de soporte de enlace	Enlace de datos-LLC	Específico del protocolo	Interfaz entre MLID y protocolo correspondiente de nivel superior
IPX-Protocolo de intercambio de paquetes de internet	Red	Direccionamiento	Red lógica Servicio
		Selección de ruta	Dinámico
		Servicios de conexión	Sin conexión
RIP-Protocolo de información del ruteador	Red	Descubrimiento de ruta	Vector de distancia
NLSP-Protocolo de servicios de enlace de Netware	Red	Descubrimiento de ruta	Estado de enlace
SPX-Protocolo de intercambio de paquetes secuenciales	Transporte	Direccionamiento	Identificador de conexión
		Desarrollo de segmento	División y combinación
		Servicios de conexión	Secuencia de segmento Control de errores Control de flujo de extremo a extremo
NCP-Protocolos centrales de Netware	Transporte	Servicios de conexión	Secuencia de segmento Control de errores Control de flujo de extremo a extremo

***Tabla 3.1** Stack de protocolos IPX/SPX y su relación con el modelo OSI, sus temas y sus técnicas*

La tabla 3.1 relaciona los protocolos con los temas y técnicas del modelo OSI que se hacen referencia en el capítulo I de esta tesis.

3.3.1.1 MLID (Controlador de interfaz de enlace múltiple)

MLID es el nombre que utiliza Novell para un controlador de tarjeta de interfaz de red. Cada MLID es un componente de *software* que se adecua a la interfaz de enlace de datos abierta (ODI) de Novell. Cada MLID puede estar vinculado a varios *stacks* a la vez, pues no está vinculado con un *stack* en particular.

3.3.1.2 LSL (Nivel de soporte de enlace)

El LSL es la interfaz entre un MLID y los distintos *stacks* de protocolos de nivel superior. El LSL interpreta el campo de identificación de protocolo de cada paquete y lo pasa al *stack* de protocolos correspondiente.

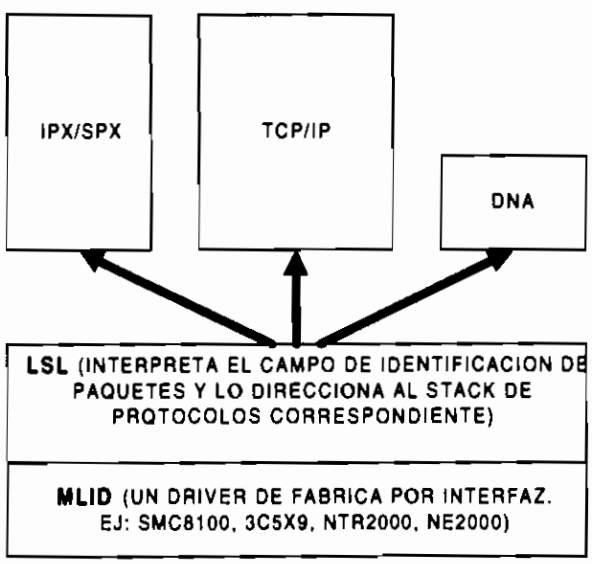


Figura 3.35 Función del protocolo LSL

3.3.1.3 IPX (Protocolo de intercambio de paquetes de internet)

IPX es un protocolo relacionado con el nivel red del modelo de referencia OSI. Es fundamentalmente un protocolo ruteable (no de enrutamiento, es decir no crea tablas de ruteo) y se encarga de direccionar y encaminar paquetes de una ubicación a otra de una internet IPX. IPX realiza funciones de encaminamiento de red lógica (direcciones lógicas) y encaminamiento de internet. Se basa en la dirección de dispositivo físico para direccionamiento de nodo, y en direcciones de servicios de nivel superior llamados zócalos para direccionar el último destino de los paquetes dentro del nodo. Además IPX selecciona la ruta basándose en la

información que le proporciona el protocolo RIP (Protocolo de información del ruteador).

3.3.1.4 RIP (Protocolo de información del ruteador)

Es un protocolo de descubrimiento de ruta (protocolo de enrutamiento que crea tablas de rutas) que utiliza vector de distancia y recuento de saltos para determinar el costo de una ruta. En ambientes Novell al protocolo RIP también se lo conoce como NRIP (*Novell RIP*) para diferenciarlo del protocolo RIP del *stack* TCP/IP o Internet.

3.3.1.5 NLSP (Protocolo de servicios de enlace de Netware)

Es un protocolo que actúa al nivel de la capa red, realiza descubrimiento de ruta basado en estado de enlace. Debido a esto, es un protocolo que ofrece tolerancia a redes de malla e híbridas.

3.3.1.6 SPX (Protocolo de intercambio de paquetes secuenciales)

Es una ampliación de IPX que permite la transmisión de paquetes de nivel transporte orientada a conexión. SPX establece circuitos virtuales llamados conexiones, y cuenta con identificadores de conexión específicos (ID de conexión) situados en la cabecera de SPX. SPX garantiza la transmisión, mediante retransmisiones en el caso de que la información no se reciba correctamente.

3.3.2 DEL *STACK* DE PROTOCOLOS TCP/IP

Este *stack* de protocolos fue desarrollado por el Departamento de Defensa de los Estados Unidos y varias organizaciones para su propio uso. Al mencionado *stack* se lo conoce también como *stack* Internet, y cuenta con una serie de protocolos de comunicación y aplicaciones, entre los cuales los más importantes (de comunicación) son TCP e IP.

Debido a que su origen fue anterior al modelo de referencia OSI con aproximadamente 10 años, su diseño fue realizado basado en un modelo propio, conocido como modelo DOD.

El **modelo de referencia DOD** ***(US. Department Of Defense***, consta de 4 capas, cada una de las cuales es responsable de realizar funciones de conectividad específicas y podría incluir algunos protocolos. La figura 3.36 muestra las capas del modelo de referencia OSI junto a sus equivalentes en el modelo DOD, y se describe además la función breve de cada una.

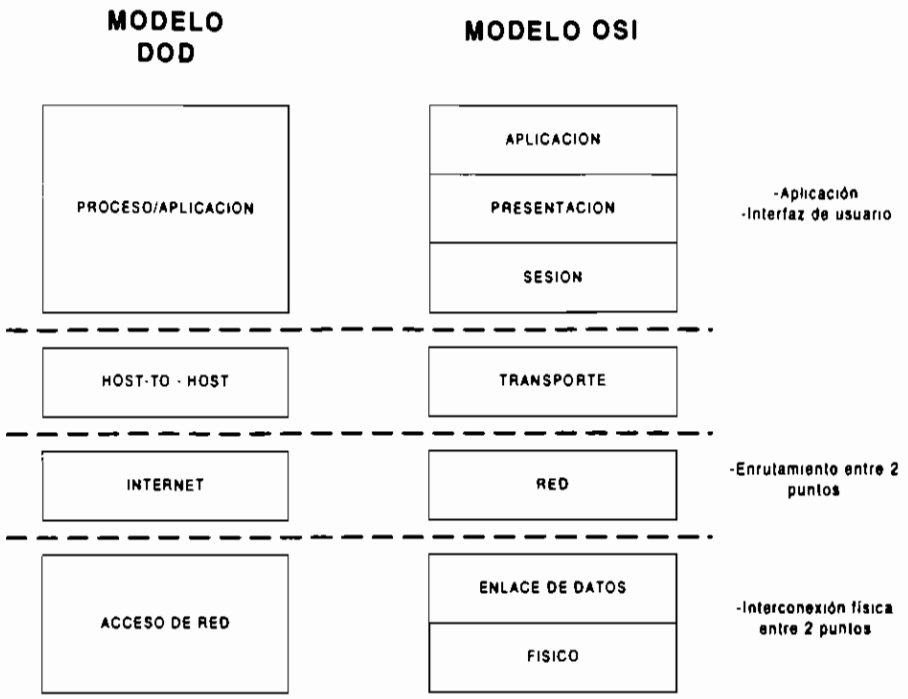


***Figura 3.36** Relación entre el modelo DOD y el modelo OSI*

En la figura 3.37 se muestra la relación de todos[27] los protocolos del *stack* TCP/IP, con el modelo de referencia OSI y DOD.

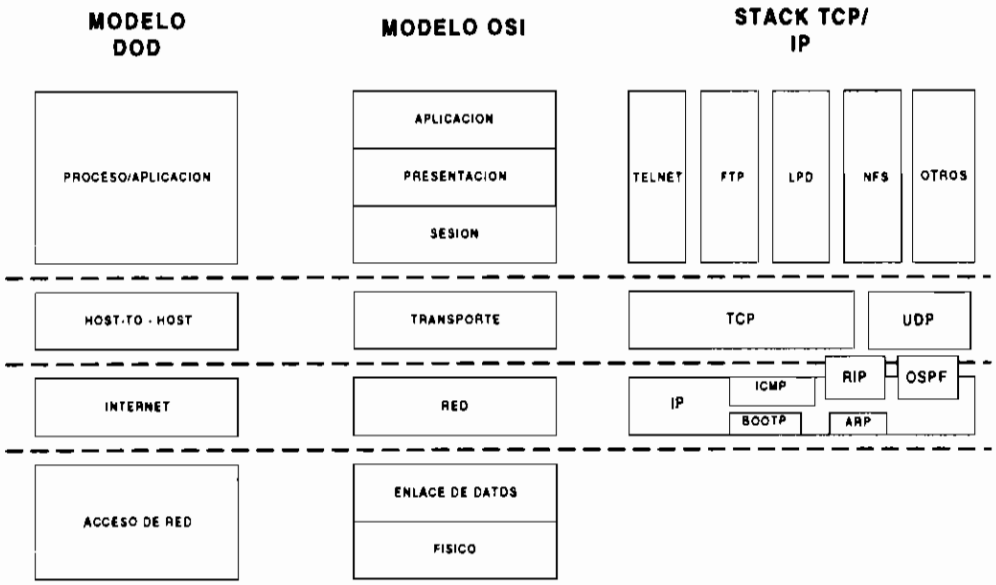


***Figura 3.37** Stack de protocolos TCP/IP y su relación con los modelos DOD y OSI*

[27] Se hace referencia a todos los protocolos del *stack*, debido a que este *stack* en particular está alcanzando su mayor difusión a escala mundial debido a la comunicación y aplicaciones que brinda dentro de la red más grande del mundo conocida como INTERNET.

La tabla 3.2 relaciona los protocolos de comunicaciones del *stack* TCP/IP con los temas y técnicas del modelo OSI que se hace referencia en el capítulo I de esta tesis. No se incluyen los protocolos de aplicaciones de este *stack*.

Protocolo	**Nivel OSI**	**Temas**	**Técnicas**
IP-Protocolo Internet	Red	Direccionamiento	Red lógica
		Conmutación	Paquete
		Selección de ruta	Dinámico
		Servicios de conexión	Control de errores
ICMP-Protocolo de mensajes de control de Internet	Red	Servicios de conexión	Control de errores Control de flujo de nivel de red
RIP-Protocolo de información del ruteador	Red	Descubrimiento de ruta	Vector de distancia
OSPF-Abrir ruta más corta primero	Red	Descubrimiento de ruta	Estado de enlace
TCP-Protocolo de control de transmisión	Red	Direccionamiento	Servicio
	Transporte	Direccionamiento	Identificador de conexión
		Desarrollo de segmento	División y combinación
		Servicios de conexión	Secuencia de segmento Control de errores Control de flujo de extremo a extremo
UDP-Protocolo de datagrama de usuario	Transporte	Direccionamiento	Identificador de conexión
		Desarrollo de segmento	Combinación
		Servicios de conexión	Sin conexión
ARP-Protocolo de resolución de direcciones	Red	Resolución de dirección	Método de resolución específico del protocolo que iguala direcciones de dispositivo lógico y físico
DNS-Sistema de nombres de dominio	Transporte	Resolución de nombre/dirección	Iniciado por el proveedor de servicio

***Tabla 3.2** Stack de protocolos IP/TCP y su relación con el modelo OSI, sus temas y sus técnicas*

3.3.2.1 IP (Protocolo Internet)

IP es una implementación de nivel de red para paquetes conmutados sin conexión que realiza direccionamiento y selección de ruta. IP también puede

fragmentar paquetes en partes más pequeñas, si lo requiere, y volver a unirlas en un anfitrión intermedio (ruteador por ejemplo) o en el destino. Cada paquete (denominado datagrama IP) dispone de una cabecera IP y se transmite como una trama mediante protocolos de nivel inferior (*Ethernet*, *Token-Ring*, FDDI por ejemplo).

IP mueve los datagramas de ruta consultando las tablas dinámicas de ruta en cada salto (ruteador). Cada ruteador toma una decisión del salto siguiente del datagrama, basándose en las direcciones de red lógica y física proporcionadas por ARP.

Además IP, proporciona una pequeña cantidad de control de errores, utilizando suma de comprobación sólo para la cabecera, pero no para los datos del nivel red.

3.3.2.2 ICMP(Protocolo de mensajes de control de internet)

Debido a que IP es un protocolo que no tiene conexión, no puede detectar condiciones de error en la red. ICMP se utiliza para notificar a IP y a protocolos de nivel superior la existencia de errores en el nivel de red y problemas de control de flujo.

3.3.2.3 RIP (Protocolo de información del ruteador)

RIP es un protocolo de descubrimiento de ruta (enrutamiento) que utiliza vector de distancia. Por esta razón, envía periódicamente sus tablas de ruta por toda la red, generando tráfico que no es recomendable en interredes grandes y complejas.

3.3.2.4 OSPF (Abrir ruta más corta primero)

Este es un protocolo de descubrimiento de ruta que utiliza estado de enlace. Por esta razón, elimina el problema de tráfico que ocurría con RIP, proporcionando mejor rendimiento que RIP en interredes grandes, ya que facilita el encaminamiento basado en la clase de servicio y balance de carga.

3.3.2.5 TCP (Protocolo de control de transmisión)

Es el protocolo de transporte primario de este *stack*. Capta mensajes de cualquier longitud de los protocolos de nivel superior y proporciona transporte totalmente dúplex orientado a conexión.

TCP acepta flujos de datos, descompone el flujo en segmentos y pasa el segmento a IP. Debido a que IP no tiene conexión, TCP debe proporcionar

sincronización de secuencia para cada segmento. TCP realiza esta tarea asignando números de secuencia en el nivel de byte. Con el fin de optimizar tiempo y ancho de banda, TCP puede combinar numerosas conversaciones del nivel superior en cada segmento. La transmisión de datagramas se realiza asignando un identificador de conexión llamado puerto o zócalo, a la conexión de cada circuito virtual.

3.3.2.6 UDP (Protocolo de datagrama de usuario)

Al igual que TCP, UDP también proporciona servicios de transporte. A diferencia de TCP, UDP no está orientado a conexión y no da reconocimiento de la recepción de datos. UTP simplemente acepta y transporta datagramas. La transmisión de datagramas de UDP también se consigue asignando una dirección de puerto. Sin embargo, el puerto solo es un puntero a un proceso local, y no una conexión de circuito virtual. Dado que no realiza funciones de establecimiento y liberación de conexiones, control de flujo y otras, UDP transfiere datos más rápido que TCP.

3.3.2.7 ARP (Protocolo de resolución de direcciones)

Este protocolo determina las direcciones de IP numéricas a partir de un nombre de nodo específico. En este *stack*, se utiliza una combinación de direcciones de dispositivo físico y red lógica de una red para formular un dirección de IP. Los nodos lógicos también pueden asignarse con nombres para hacer referencia al mismo nodo y facilitar de esta forma la interacción humana.

3.3.2.8 DNS (Sistema de nombres de dominio)

Es un sistema de base de datos distribuida que realiza resolución de dirección/nombre en beneficio de las aplicaciones del cliente. Los servidores DNS mantienen la estructura jerárquica de nombres, de tal forma que los anfitriones individuales pueden utilizar nombres lógicos para una fácil identificación humana.

3.3.3 DEL *STACK* DE PROTOCOLOS DNA (*DIGITAL NETWORK ARCHITECTURE*)

DNA es una arquitectura creada por *Digital Equipment Corporation* (DEC). Recientemente DNA se ha centrado en el medio de estándares ISO basados en el modelo de referencia OSI. Por esta razón DNA coincide en gran medida con el modelo de referencia OSI, tal como se observa en el siguiente gráfico:

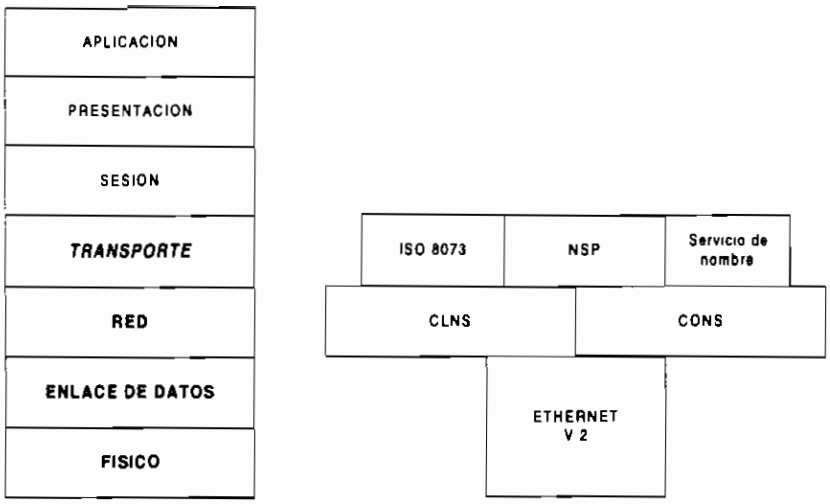


Figura 3.38 Stack de protocolos DNA y su relación con el modelo OSI

La tabla 2.3 relaciona los protocolos de comunicaciones para LAN del *stack* DNA con los temas y técnicas del modelo OSI que se hacen referencia en el capítulo I de esta Tesis. No se incluyen los protocolos de aplicaciones de este *stack.*

3.3.3.1 *Ethernet* V.2

Es un protocolo del nivel físico y de enlace de datos de 10 Mbps, utiliza CSMA/CD y codificación Manchester, a través de cable coaxial. Es la base de diseño y es muy similar a la familia de protocolos IEEE/ISO 802.X/8802.X, pero con un formato de trama ligeramente distinto.

3.3.3.2 CLNS (Servicio de red sin conexión)

Es un protocolo del nivel de red con servicios de red sin conexión (OSI CLNS) y con conexión (OSI CONS). Sin embargo, DNA fase V utiliza CLNS, que se basa en los 3 protocolos ISO siguientes:

- ISO 8473, protocolo de prestación de servicios sin conexión. Controla las tareas de transmisión de datos entre dos sistemas terminales.
- ISO 9542, protocolo de intercambio de encaminamiento de sistema final a intermedio para prestación de servicios de red sin conexión, utilizado para realizar funciones de encaminamiento.
- ISO 10589, protocolo de intercambio de encaminamiento intradominio de sistema intermedio a sistema intermedio para uso con el protocolo para prestación de servicio de red sin conexión, que define los mecanismos para mover paquetes de datos entre ruteadores.

Debido a que estos protocolos proporcionan servicio sin conexión, se limitan a realizar tareas de direccionamiento, conmutación, descubrimiento y selección de ruta.

Protocolo	Nivel OSI	Temas	Técnicas
Ethernet V.2	Físico	Tipos de conexión	Multipunto
		Topología física	Bus
		Señalización digital	Transición de estado
		Sincronización de bit	Sincrónico
		Uso del ancho de banda	Banda base
	Enlace de datos MAC	Topología lógica	Bus
		Acceso al medio	Contención
		Direccionamiento	Dispositivo físico
CLNS (ISO 8473, 9542 Y 10589) Servicio de red sin conexión	Red	Direccionamiento	Red lógica
		Descubrimiento de ruta	Estado de enlace
		Selección de ruta	Dinámico
CONS (ISO 8878 y 8208)- Servicio de red con conexión	Red	Direccionamiento	Red lógica
		Descubrimiento de ruta	Estado de enlace
		Selección de ruta	Dinámico
		Servicios de conexión	Control de flujo del nivel de red Control de errores Control de secuencia de paquetes
ISO 8073, especificación de protocolo de transporte orientado a conexión	Transporte	Direccionamiento	Identificador de conexión
		Servicios de conexión	Secuencia de segmento Control de errores Control de flujo de extremo a extremo
NSP-Protocolo de servicio de direcciones	Transporte	Direccionamiento	Identificador de conexión
		Servicios de conexión	Secuencia de segmento Control de errores Control de flujo de extremo a extremo

***Tabla 3.3** Stack de protocolos DNA y su relación con el modelo OSI, sus temas y sus técnicas*

3.3.3.3 NSP (Protocolo de servicio de red)

Ofrece un servicio controlado por flujo y orientado a conexión por medio de subcanales totalmente dúplex normales o acelerados. Para conseguir control de flujo de extremo a extremo, el nivel de red informa sobre la existencia de congestión en el NSP transmisor, reduciendo el número de mensajes pendientes que tolera y utilizando el método de tasa garantizada o de control de flujo de ventanas.

3.3.3.4 ISO 8073, Especificación de protocolo de transporte orientado a conexión

Utilizado para proporcionar una conexión fiable en el nivel de transporte. Su implementación determina el nivel de control de flujo, errores y secuencia de paquetes que proporciona la red.

3.3.4 DEL *STACK* DE PROTOCOLOS *APPLE TALK*

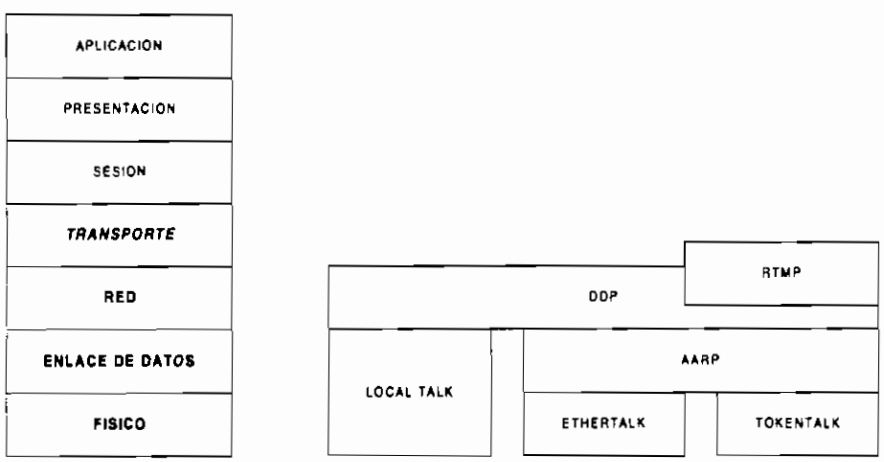


***Figura 3.39* Stack de protocolos Apple Talk y su relación con el modelo OSI**

Esta serie de protocolos se creó como la arquitectura de red para computadores Macintosh. En la actualidad, *Apple Talk* proporciona conectividad para sistemas PC IBM con MS-DOS, *mainframes* IBM, Digital Equipment VAX y varios computadores UNIX.

El *stack* de protocolos *Apple Talk*, nació luego de la existencia del modelo de referencia OSI, y su diseño fue realizado basándose en el mencionado modelo, razón por la cual la estratificación de los protocolos del *stack* coincide en gran medida con la estratificación del modelo.

En la tabla 3.4 se muestra la relación de los protocolos de comunicaciones para LAN del *stack Apple Talk* con los temas y técnicas del modelo OSI que se hacen referencia

en el capítulo I de esta Tesis. No se incluyen los protocolos de aplicaciones de este *stack*.

Protocolo	Nivel OSI	Temas	Técnicas
LocalTalk	Físico	Tipos de conexión	Multipunto
		Topología física	Bus
		Señalización digital	Transición de estado
		Sincronización de bits	Sincrónico
		Uso del ancho de banda	Banda base
	Enlace de datos MAC	Topología lógica	Bus
		Acceso al medio	Contención
		Direccionamiento	Dispositivos físico
	Enlace de datos LLC	Sincronización de transmisiones	Sincrónico
		Servicios de conexión	Control de flujo LLC Control de errores
AARP-Protocolo de resolución de direcciones *Apple Talk*	Enlace de datos de red	Resolución de direcciones	Método de resolución específico del protocolo que iguala direcciones de dispositivo lógico y físico
DDP-Protocolo de transmisión de datagrama	Red	Direccionamiento	Red lógica Servicio
		Selección de ruta	Dinámico
		Servicio *gateway*	Traducción del nivel de red
RTMP-Protocolo de mantenimiento de tablas de ruta	Red	Descubrimiento de ruta	Vector de distancia

***Tabla 3.4** Stack de protocolos Apple Talk y su relación con el modelo OSI, sus temas y sus técnicas*

3.3.4.1 *LocalTalk, EtherTalk, TokenTalk* (LLAP, ELAP, TLAP)

LocalTalk Link Acces Protocol (conocido como LLAP) es un protocolo CSMA/CD específico de Apple para medio de transmisión de par trenzado blindado. Debido a que trabaja con segmentos limitados a 300 metros, con un máximo de 32 dispositivos y velocidades de 230,4 Kbps, es conveniente para grupos de trabajo pequeños. Una de sus mejores características es que permite la asignación automática de direcciones. Durante el inicio de conexión cada

dispositivo negocia con el resto de dispositivos activos una dirección aceptable de dispositivo físico.

EtherTalk (llamado también ELAP) y *TokenTalk* (llamado también TLAP) son simplemente implementaciones de protocolos *Apple Talk* que utilizan protocolos *Ethernet* y *Token-Ring*.

3.3.4.2 AARP (Protocolo de resolución de direcciones *Apple Talk*)

Dado que ELAP y TLAP utilizan direcciones de dispositivo físico predefinidas, *Apple Talk* utiliza AARP para asignar direcciones *Apple Talk* a las direcciones físicas predefinidas de ELAP y TLAP. AARP permite que los niveles superiores de *Apple Talk* funcionen con diversos protocolos del nivel de enlace de datos.

3.3.4.3 DDP (Protocolo de entrega de datos)

Es un protocolo primario del nivel red. Proporciona servicio sin conexión entre dos zócalos (direcciones de servicio).

DDP utiliza la dirección completa para encaminar paquetes a través de la red. DDP se basa en las tablas de ruta proporcionadas por RTMP para determinar el salto siguiente de enrutamiento. Cuando se alcanza el ruteador de la red de destino, la implementación de nivel de datos transmite el paquete localmente.

3.3.4.4 RTMP (Protocolo de mantenimiento de tablas de ruta)

Es un protocolo de descubrimiento de ruta para crear y mantener tablas de encaminamiento *Apple Talk*. Utiliza un algoritmo de encaminamiento de vector de distancia similar a RIP.

3.3.5 DEL *STACK* DE PROTOCOLOS SNA (*SYSTEM NETWORK ARCHITECTURE*)

SNA es una arquitectura de red proporcionada por IBM que se basó en un modelo propio de SNA. SNA no define un único *stack* de protocolos, sino que describe las características generales del *hardware* y *software* de computador que se necesita para la interconexión. Esta serie de protocolos fue el fundamento del modelo de referencia OSI que fue establecido aproximadamente 10 años después.

En la figura 3.40 se muestran los dos modelos SNA y OSI junto al *stack* de protocolos SNA.

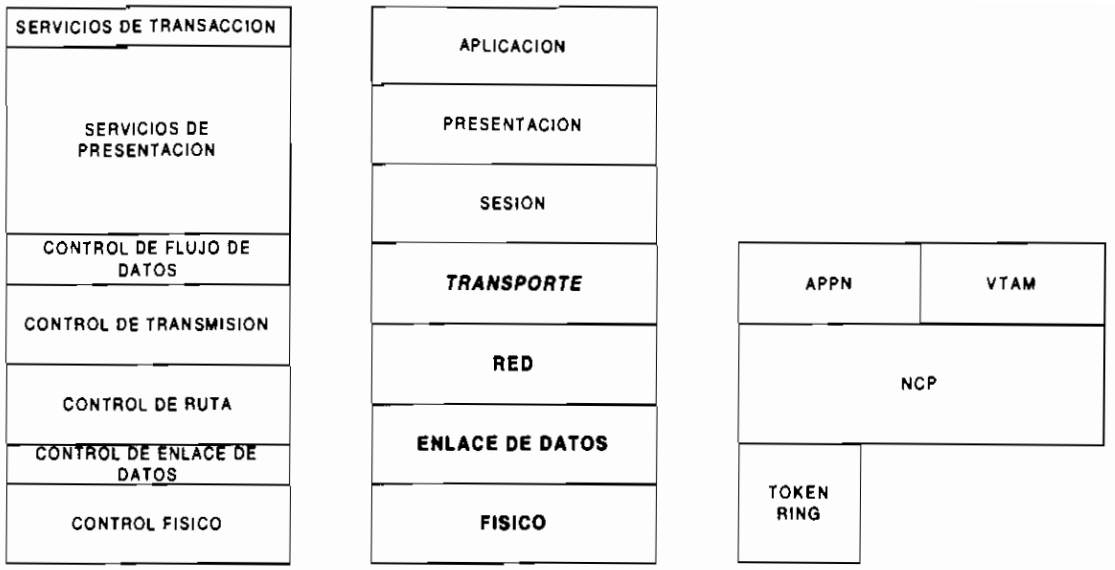


***Figura 3.40** Stack de protocolos SNA y su relación con el modelo OSI y SNA*

En la tabla 3.5 se muestra la relación de los protocolos de comunicaciones para LAN del *stack* SNA con los temas y técnicas del modelo OSI que se hacen referencia en el capítulo I de esta Tesis. No se incluyen los protocolos de aplicaciones de este *stack* ni los considerados protocolos WAN.

3.3.5.1 *Token-Ring*

Es la especificación LAN de IBM que sirvió de modelo para IEEE 802.5 con la excepción de que *Token-Ring* especifica una topología física radial. *Token-Ring* utiliza un método de acceso al medio de entrega de testigo para proporcionar una velocidad de 4 y 16 Mbps.

3.3.5.2 NCP (Programa de control de red)

Es un producto de IBM que controla recursos conectados a un control de comunicaciones. Fue diseñado para operar procesadores de preprocesamiento y realizar funciones de enlace de datos y funciones limitadas de nivel de red. En la actualidad NCP proporciona funcionabilidad de encaminamiento y *gateway* en redes SNA.

3.3.5.3 VTAM (Método de acceso virtual de telecomunicaciones)

Se encarga del control de comunicación y flujo de datos en redes SNA. VTAM trabaja con NCP para controlar los recursos de la red.

Protocolo	Nivel OSI	Temas	Técnicas
Token-Ring	Físico	Tipo de conexión	Punto a punto
		Topología física	Radial
		Señalización digital	Transición de estado
		Sincronización de bit	Sincrónico
		Uso del ancho de banda	Banda base
	Enlace de datos MAC	Topología lógica	Anillo
		Acceso a medios	Entrega de testigo
		Direccionamiento	Dispositivo físico
NCP-Programa de control de red	Enlace de datos-MAC	Acceso al medio	Sondeo
		Direccionamiento	Dispositivo físico
	Enlace de datos-LLC	Servicios de conexión	Control de flujo
	Red	Direccionamiento	Red lógica
		Selección de ruta	Estático
		Servicios de *gateway*	Traducción del nivel de red
VTAM-Método de acceso virtual a telecomunicaciones	Transporte	Direccionamiento	Identificador de conexión
		Desarrollo de segmento	División y combinación
		Servicios de conexión	Control de flujo de extremo a extremo
APPN-Conectividad avanzada par a par	Red	Direccionamiento	Red lógica
	Transporte	Servicios de conexión	Secuencia de segmento Control de flujo de extremo a extremo

***Tabla 3.5** Stack de protocolos SNA y su relación con el modelo OSI, sus temas y sus técnicas*

3.3.5.4 APPN (Conectividad avanzada par a par)

Es un protocolo de los niveles red y transporte que permite que SNA opere redes que sólo utilizan PU[28] tipo 2.1 (minicomputadores, controladores de ensamble, y estaciones de trabajo que pueden comunicarse con un *mainframe* u otros dispositivos de su mismo tipo) sin *mainframes*. APPN proporciona descubrimiento de ruta, servicios de directorio y control de flujo de ventanas.

[28] PU (*Physical Unit*)

3.3.6 PROTOCOLOS DE LA SERIE IEEE 802.X

El Instituto de Ingenieros Eléctricos y Electrónicos (IEEE) publicó una serie de estándares del nivel físico y de enlace de datos (realizados por el comité 802) que adoptó el Instituto Nacional Norteamericano de Estándares (ANSI). Posteriormente ISO revisó y reeditó estos estándares pasando a llamarse protocolos ISO 8802. Debido a la semejanza de los estándares IEEE 802 e ISO 8802, solo se revisarán los estándares publicados por la IEEE.

La mayoría de estos estándares coinciden con el modelo de referencia OSI y son también en su mayoría protocolos de redes LAN, aunque muchos de ellos pueden aplicarse también en redes WAN.

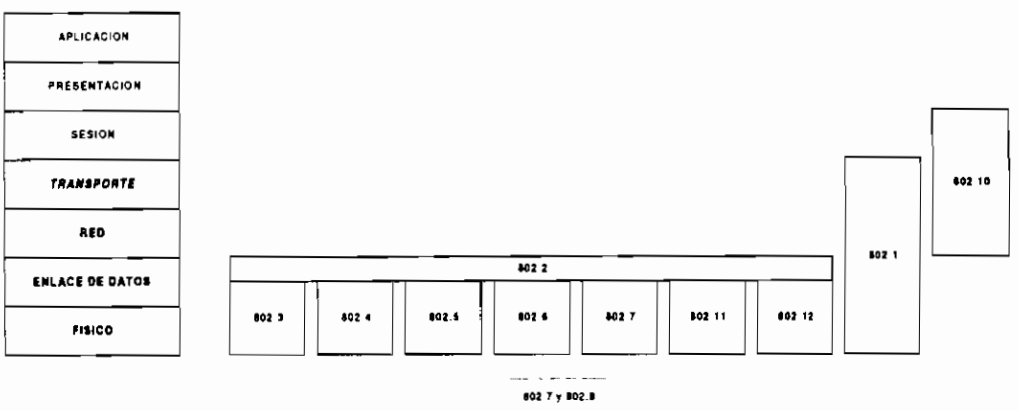


Figura 3.41 Protocolos 802.X y su relación con el modelo OSI

Protocolo	Nivel OSI	Temas	Técnicas
802.2	Enlace de datos LLC	Específico del protocolo	Identificación de protocolos de nivel superior
802.3 (salvo que se indique lo contrario)	Físico	Tipos de conexión	Multipunto
		Señalización digital	Transición de estado
		Sincronización de bit	Sincrónico
		Uso del ancho de banda	Banda base (Excepto 10BROAD36)
	Enlace de datos MAC	Topología lógica	Bus
		Acceso a medios	Contención
		Direccionamiento	Dispositivo físico
802.3 1BASE5	Físico	Topología física	Radial
802.3 10BASE2	Físico	Topología física	Bus
802.3 10BASE5	Físico	Topología física	Bus
802.3 10BASET	Físico	Topología física	Radial
802.3 10BASEF	Físico	Topología física	Radial

802.3 10BROAD36	Físico	Topología física	Bus
		Uso del ancho de banda	Banda ancha
802.4	Físico	Tipos de conexión	Multipunto
		Topología física	Bus
		Señalización digital	Transición de estado
		Sincronización de bit	Sincrónico
		Uso del ancho de banda	Banda base
	Enlace de datos MAC	Topología lógica	Anillo
		Acceso al medio	Entrega de testigo
		Direccionamiento	Dispositivo físico
802.5	Físico	Tipos de conexión	Punto a punto
		Topología física	Anillo
		Señalización digital	Transición de estado
		Sincronización de bit	Sincrónico
		Uso del ancho de banda	Banda base
	Enlace de datos MAC	Topología lógica	Anillo
		Acceso al medio	Entrega de testigo
		Direccionamiento	Dispositivo físico
802.6	Físico	Tipos de conexión	Punto a punto
		Topología física	Anillo
		Uso del ancho de banda	Banda base
	Enlace de datos MAC	Topología lógica	Anillo
802.11	Enlace de datos MAC	Acceso al medio	Contención
802.12	Físico	Tipos de conexión	Multipunto
		Topología física	Radial
		Uso del ancho de banda	Banda base
	Enlace de datos MAC	Topología lógica	Bus
		Acceso al medio	Contención

***Tabla 3.6** Protocolos de la serie 802.X y su relación con el modelo OSI, sus temas y sus técnicas*

3.3.6.1 IEEE 802.2

Es un estándar del nivel de enlace de datos para uso con implementaciones 802.3, 802.4, 802.5 y 802.6. IEEE 802.2 agrega varios campos de cabecera a los

que emplean normalmente los protocolos inferiores. Estos campos identifican qué protocolo de nivel superior se utiliza en la trama y qué procesos del nivel de red son el origen y destino de la trama.

3.3.6.2 IEEE 802.3

Es el estándar *Ethernet* propuesto por IEEE, el cual ofrece varias opciones de nivel físico, incluidos modos de señalización distintos (banda base y banda ancha), tipos de medio, topologías y velocidades de transmisión de datos. El elemento común a estas opciones es el método de acceso al medio CSMA/CD.

Las implementaciones individuales tienen nombres que utilizan una convención de tres partes. La primera es un número que representa la velocidad de transmisión en Mbps. La segunda indica BASE para banda base y BROAD para banda ancha. La tercera indica la distancia efectiva aproximada o se utiliza como un designador especial.

Son aceptadas las siguientes especificaciones[29]:

- ***1BASE5*** utiliza cable UTP de calibre 24 para manejar una señal de banda base de 1 Mbps para distancias de hasta 500 metros (250 metros por segmento) en una topología física radial.
- ***10BASE2*** utiliza cable coaxial (RG58) de 5 mm y 50 ohmios para manejar una señal de banda base de 10 Mbps para distancias de segmento de hasta 185 metros en una topología física de bus (la cual se denomina "*Ethernet* fina")
- ***10BASE5*** utiliza cable coaxial de 10 mm y 50 ohmios para manejar una señal de banda base de 10 Mbps para distancias de segmento de hasta 500 metros en una topología física de bus (la cual se denomina "*Ethernet* gruesa")
- ***10BASE-T*** utiliza cable UTP 24 AWG para manejar una señal de banda base de 10 Mbps para distancias de hasta 100 metros en una topología física radial.
- ***10BASE-F*** utiliza cable de fibra óptica para manejar una señal de banda base de 10 Mbps para distancias de hasta 4 Km en una topología física radial. Existen 3 especificaciones: 10BASE-FL para enlace de fibra, 10BASE-FB para segmento principal de fibra y 10BASE-FP para pasivo de fibra.
- ***10BROAD36*** utiliza cable coaxial de 75 ohmios para manejar una señal de banda ancha de 10Mbps para distancias de hasta 1800 metros (o 3600 si se utilizan cables dobles) en una topología física de bus.

3.3.6.3 IEEE 802.4

Este estándar se creó para satisfacer las necesidades de LAN en la automatización de fábricas e industrias. Establece una topología en bus, con

[29] Actualmente se habla del estándar 802.3z correspondiente a Gigabit Ethernet, pero se presume que su aceptación oficial como estándar será en el primer cuarto de 1998. Gigabit Ethernet es semejante a Fast Ethernet, pero 10 veces más rápido.

método de acceso a medios de entrega de testigo, banda base y ancha sobre cable coaxial de 75 ohmios o fibra óptica.

3.3.6.4 IEEE 802.5

Este estándar se basa en la especificación *Token-Ring* de IBM. Utiliza un método de acceso a medios de entrega de testigo y codificación diferencial Manchester para proporcionar velocidades de 1, 4 ó 16 Mbps. Su diferencia con *Token-Ring* es que no necesita un medio de transmisión ni una topología física específica.

3.3.6.5 IEEE 802.6

En este estándar se eligió y seleccionó una tecnología llamada *Distributed Queue Dual Bus* (DQDB) para uso en implementaciones MAN. DQDB utiliza una topología de bus doble basada en fibra que puede configurarse en bucle para tolerancia a fallos. Cada bus es unidireccional y los dos buses funcionan en direcciones opuestas. DQDB asigna dinámicamente ancho de banda por medio de un sistema de acceso de división de tiempo. El tráfico puede ser sincrónico o asincrónico, pudiendo por tanto, realizarse transmisiones de voz, video y datos.

3.3.6.6 IEEE 802.9

Es un *Ethernet* isocrónico (también llamado IsoEnet) que proporciona una velocidad de transmisión de datos de 16 Mbps mediante una combinación de canal asíncrono de 10 Mbps con 96 canales dedicados de 64 Kbps (6 Mbps) sobre UTP. Está diseñado para redes LAN con tráfico en ráfagas y sensible al tiempo.

3.3.6.7 IEEE 802.11

Está desarrollándose para implementaciones de LAN sin cable (LAN wireless).

3.3.6.8 IEEE 802.12

Es un nuevo estándar de 100 Mbps conocido como 100 VG AnyLAN. Se basa en una propuesta de AT&T, IBM y Hewlett-Packard para una red de topología física radial basada en contención. A diferencia de los sistemas de contención típicos, en este estándar se competirá por el acceso al medio señalizando un concentrador. Cuando se produzcan peticiones simultáneas, el concentrador otorgará derechos de transmisión evaluando la prioridad de cada transmisión, dando el control del medio al dispositivo de más alta prioridad. IEEE 802.12 admiten tipos de trama *Ethernet* y *Token-Ring*.

3.3.7 PROTOCOLOS DE ALTA VELOCIDAD

Debido a que cada día más PCs con conectadas a redes y al avance tecnológico en cuanto a microprocesadores, métodos de almacenamiento de disco, memoria, etc, y al decremento en sus precios, las LANs deben estar preparadas para aplicaciones que exigen grandes recursos.

Si bien no todos los usuarios requieren emplear la red de 100 Mbps, muchas aplicaciones de datos intensivas de LAN ya han alcanzado el límite de las LANs existentes de 10 y 16 Mbps. Las mencionadas aplicaciones de datos intensivas (tales como videoconferencia, multimedia, groupware, bases de datos cliente servidor, etc) pueden beneficiarse de las tecnologías de 100 Mbps y más.

3.3.7.1 FDDI (Interfaz de datos distribuidos por fibra)

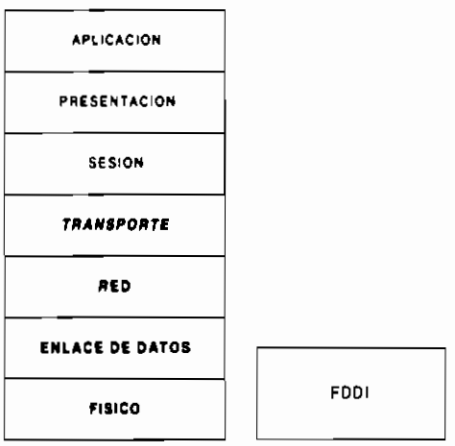


***Figura 3.42** FDDI y su relación con el modelo OSI*

FDDI fue desarrollado por el comité X3T9.5 de ANSI. Luego fue también adoptado por ISO como estándar 9314.

FDDI incluye especificaciones del nivel físico y de enlace de datos MAC. Fue diseñado para que sus servicios sean utilizados principalmente con IEEE 802.2, pero puede soportar otros protocolos de nivel superior.

Protocolo	Nivel OSI	Temas	Técnicas
FDDI	Físico	Tipos de conexión	Punto a punto
		Topología física	Radial Anillo doble
		Señalización digital	Transición de estado
		Uso del ancho de banda	Banda base
	Enlace de datos MAC	Topología lógica	Anillo
		Acceso de medio	Entrega de testigo

***Tabla 3.7** Protocolo FDDI y su relación con el modelo OSI, sus temas y sus técnicas*

FFDI es un protocolo de 100 Mbps que funciona sobre una topología física de doble anillo y una topología lógica en anillo con entrega de testigo, con especificaciones que soportan tanto fibra óptica como cable de par trenzado. Por utilizar un método de acceso al medio de entrega de testigo, FDDI es determinística. Como se ve, es muy semejante a IEEE 802.5, con ventajas en cuanto a velocidad de transmisión y distancias efectivas mayores.

FDDI se basa en anillos dobles para permitir redundancia en caso de fallas. Sólo un anillo es utilizado en situaciones normales. Si se produce una falla, el anillo se interrumpe en un nodo o concentrador de red conectado físicamente a ambos anillos (a estos dispositivos se los conoce como DAS[30]), y posteriormente el camino es redireccionado ocupando también el camino redundante

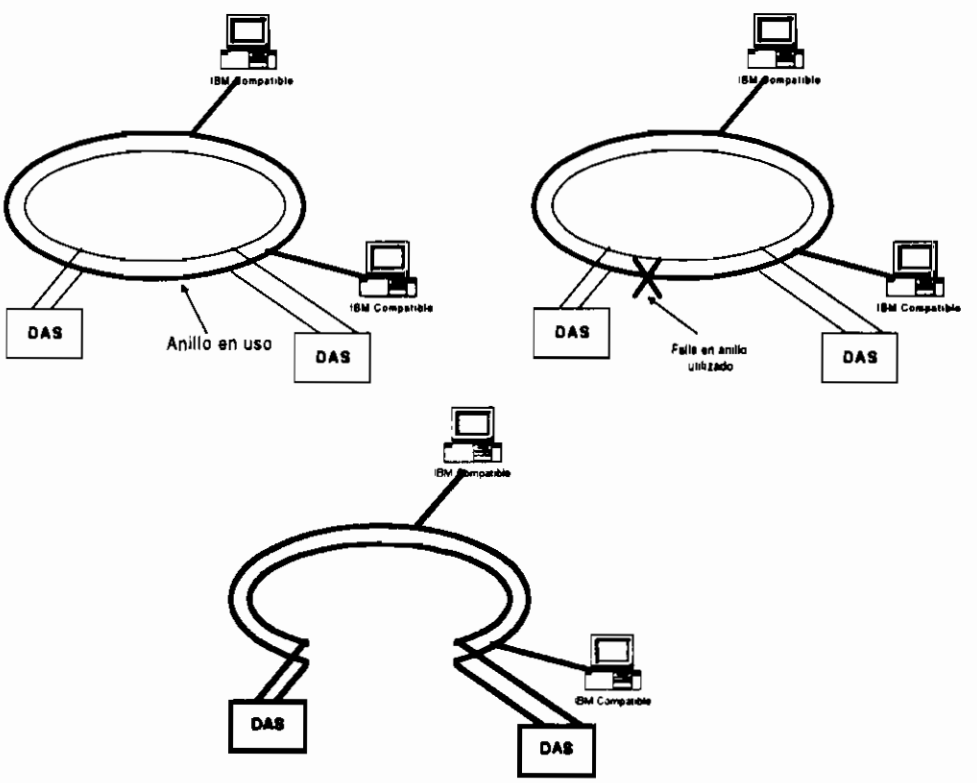


***Figura 3.43* Recuperación de fallas en una topología de doble anillo**

Existe también la versión de FDDI pero sobre cable de cobre (que es más barato) a la cual se la conoce como CDDI *(Copper Distributed Data Interface).*

Actualmente, FDDI es un protocolo de red que todavía sigue utilizándose especialmente al nivel de *backbone*, pero está siendo desplazado por otros protocolos de alta velocidad.

[30] DAS *(Dual-Attached Station).* También conocida como estación clase A, es un dispositivo conectado a los dos anillos FDDI de una red. Si el primer anillo falla, la estación puede usar el segundo.

3.3.7.2 *Fast Ethernet*[31]

Protocolo	Nivel OSI	Temas	Técnicas
Fast Ethernet	Físico	Tipos de conexión	Multipunto
		Señalización digital	Transición de estado
		Sincronización de bit	Sincrónico
		Uso del ancho de banda	Banda base
	Enlace de datos MAC	Topología lógica	Bus
		Acceso a medios	Contención
		Direccionamiento	Dispositivo físico

***Tabla 3.8** Protocolo Fast Ethernet y su relación con el modelo OSI, sus temas y sus técnicas*

Las principales ventajas que ofrece *Fast Ethernet* son las siguientes:

- Alto rendimiento
- Tecnología basada en estándares
- Costo efectivo de migración con máximo uso de equipo existente, infraestructura de transporte y sistemas de administración de red.
- Soporte de proveedores líderes en todas las áreas de productos de conectividad
- Valor óptimo

A. Alto rendimiento

Una de las principales razones para elegir *Fast Ethernet* para grupos de trabajo, es la habilidad que tiene para manejar requerimientos normales de LAN, así como para soportar los grandes picos de carga de trabajo provocados por PCs de alto rendimiento y sofisticación así como por las aplicaciones de uso intensivo de ancho de banda. Cuando se tienen transmisiones de datos con ráfagas de alta velocidad, *Fast Ethernet* es una buena elección.

B. Tecnología basada en estándares

Fast Ethernet fue diseñada como una extensión de 10BASE-T *Ethernet*. La tecnología *Fast Ethernet* también está basada sobre CSMA/CD MAC. Este protocolo también es desarrollado por el comité IEEE 802.3, el mismo que desarrolló 10BASE-T.

Es decir, 100BASE-T es una *Ethernet* convencional, solamente que más rápida. Posee la misma confiabilidad, es igualmente robusta y además tecnológicamente económica.

Además, las dos tecnologías pueden ofrecer conexiones *Ethernet* compartidas o conmutadas.

[31] *Gigabit Ethernet* (802.3z), está propuesto como futuro estándar semejante en características a *Fast Ethernet* pero 10 veces más rápido.

Las conexiones compartidas proveen un total de 10 ó 100 Mbps a todas las estaciones conectadas al *hub*. Ellas son ideales para un grupo de trabajo de tamaño mediano con demandas de ancho de banda ocasionalmente altas. Tienen bajo costo.

Las conexiones conmutadas proveen máximo ancho de banda a cada puerto del *hub* conmutado. Es muy recomendable en grandes grupos de trabajo con demanda que excede los 100 Mbps.

C. Costo efectivo de migración

La gran semejanza entre 100BASE-T y 10BASE-T hace posible que la migración de 10 a 100 sea relativamente sencilla, manteniendo la infraestructura existente:

- Cable de LAN: Las especificaciones medias de 100BASE-T (100BASE-TX, 100BASE-FX y 100BASE-T4) permiten a *Fast Ethernet* correr sobre el cableado común *Ethernet* que incluyen categorías 3, 4, 5[32] de cable UTP, así como STP y fibra.
- Herramientas administrativas: Los administradores pueden mantener sus herramientas de análisis de red y procedimientos en ambientes 100BASE-T. La información administrativa se traslada fácilmente de *Ethernet* 10BASE-T a *Fast Ethernet*.
- *Software* de administración: Las LANs *Fast Ethernet* pueden administrarse con protocolos SNMP y MIB.
- Soporte de *software*: El *software* de aplicaciones y de red funcionará sin cambios sobre 100BASE-T.
- Migración flexible: Adaptadores auto configurables a 10 ó 100 Mbps (10/100 Mbps)[33]. De manera similar, conmutadores *Ethernet* (10-100 Mbps)[34] y (10/100 Mbps).

D. Soporte de proveedores

100BASE-T ya tiene soporte en la industria, en compañías miembros de la FEA (*Fast Ethernet* Alliance) tales como 3Com, Intel, SMC, Sun Microsystems, SynOptics y otras.

E. Valor óptimo

Debido a que la estandarización está progresando rápidamente y los productos comienzan a ser disponibles de una amplia variedad de proveedores, la relación costo/beneficio de *Fast Ethernet* es muy competitiva con las otras tecnologías de alta velocidad.

---

[32] Se pueden obtener velocidades de transmisión de 100 Mbps sobre cable UTP categoría 3 y 4, siempre y cuando se utilicen los 4 pares del cable. Para esto existe la especificación 100BaseT4 por ejemplo. Sin embargo, esta práctica no es recomendale.

[33] 10/100 Mbps. Significa que un puerto puede soportar 10 y 100 Mbps.

[34] 10-100 Mbps. Significa que hay soporte para 10 y 100 pero no sobre el mismo puerto.

3.3.7.3 ATM (Modo de Transferencia Asincrónico)

Debido a que en la década de los 80 muchas redes de área local estaban basadas en medios compartidos para transmisión de datos, pero conectadas sobre redes telefónicas públicas (de un ancho de banda dedicado y optimizadas para tráfico de voz), el CCITT ahora conocido como ITU (Unión Internacional de Telecomunicaciones), formó un grupo de estudio para investigar el concepto de *redes* integradas de alta velocidad que puedan manejar uniformemente voz, datos y una variedad de otros servicios. Como resultado de las investigaciones, surgió el protocolo para WAN llamado *BISDN (Broadband Integrated Services Digital Networks)*. Los servicios de BISDN requieren canales de alta velocidad para transmisión digital de voz, video, datos y tráfico de multimedia. ATM es la tecnología de conmutación y multiplexión para soportar servicios BISDN.

Como puede deducirse, ATM se originó inicialmente como un protocolo orientado a WAN, pero que poco a poco ha llegado a ser útil tanto a MAN como a LAN, llegando en este momento hasta la estación de trabajo.

Protocolo	Nivel OSI	Temas	Técnicas
ATM	Enlace de datos LLC	Sincronización de transmisiones	Isocrónico
		Servicios de conexión	Control de errores
	Red	Conmutación	Paquete (llamados celdas, que son paquetes de tamaño fijo que siguen un circuito virtual)
		Selección de ruta	Estático

***Tabla 3.9** Protocolo ATM y su relación con el modelo OSI, sus temas y sus técnicas*

A. El reto de ATM

Uno de los principales desafíos de ATM, fue determinar una estructura que pueda manejar eficientemente cualquier tipo de tráfico. Tal estructura debería ser capaz de manejar una variedad de tasas de bits y soportar comunicaciones en ráfagas, desde tráfico de voz, video y datos.

Mientras más gente asume que el tráfico de voz en circuitos conmutados no es en ráfagas, la energía acústica generada por una conversación está presente solamente en alrededor del 40 por ciento del tiempo. Los sistemas de transmisión telefónicos bajo el mar han doblado su capacidad de voz para por años explotar este factor y permitir que cada circuito de voz transmita solamente durante períodos activos.

La conmutación de paquetes ha sido la tecnología de elección para tráfico de datos en ráfagas, porque aquel consume ancho de banda solamente cuando el tráfico está

presente. Pero los mecanismos de conmutación de paquetes tradicionales no pueden alcanzar el rendimiento y velocidad requeridos para tiempo real, en tráfico de doble vía. ATM sobrepasa esta limitación ofreciendo paquetes con longitud fija. Cada paquete ATM, llamado *celda*, consiste de 48 bytes de carga útil y 5 bytes de cabecera. Las celdas con longitud fija ofrecen algunas ventajas:

- Las demoras de encolamiento en conectividad y conmutación son más predecibles. Los proveedores de conmutación pueden poner mecanismos para asegurar el nivel apropiado de servicio a todos los tipos de tráfico, especialmente para servicios sensitivos a la demora tales como voz y video.
- Procesar celdas ATM es menos complejo y más confiable que procesar paquetes de longitud variable. Debido a que es altamente predecible, el *hardware* de ATM permite ser implementado más eficientemente, debido a que las estructuras de control, *buffers* y esquemas de administración de *buffers* pueden ser diseñados de acuerdo a criterios de tamaño conocidos.
- Las celdas de longitud fija permiten que los conmutadores de demora de celda puedan procesar celdas en paralelo, para velocidades que excedan las limitaciones de arquitecturas de conmutadores basadas en bus.

Como los paquetes de datos tradicionales, las celdas ATM requieren ancho de banda solamente cuando el tráfico está presente, pudiendo proveer el equivalente de un *slot* de tiempo de un multiplexor de división de tiempo para tráfico continuo como la voz digitalizada. Como un resultado, ATM puede manejar tráfico de LAN en tiempo real así como tráfico en ráfagas igual de bien.

El uso eficiente del ancho de banda no es el único problema enfrentado por ATM. Diferentes tipos de tráfico requieren diferente comportamiento de demora, variación de espera y características de pérdida. Para accesar a la red una estación requiere un circuito virtual entre los terminales de transmisión y recepción. Durante la configuración de conexión la estación final puede requerir la calidad de servicio que necesita para satisfacer necesidades de transmisión, y los conmutadores ATM otorgarán los requerimientos de red suficientes que estén disponibles. La calidad de servicio garantizada del acceso conmutado basado en celdas es particularmente útil para transporte en tiempo real, y comunicación interactiva tal como la voz y el video.

En resumen, los estándares de ATM identifican cuatro clases de servicios sobre los que pueden operar los protocolos de nivel superior:

- Tráfico constante de tasa de bit
- Datos variables de paquetes de bits que deben transmitirse con demora fija
- Datos orientados a conexión
- Datos sin conexión

Cada clase de servicio se optimiza para un tipo distinto de flujo de datos (por ejemplo, la clase constante de tasa de bits acepta video, mientras que la clase de sin conexión es más adecuada para grandes transferencias de datos binarios intermitentes.

B. Los dispositivos de borde

Todas las decisiones sobre el manejo de tráfico ATM están basadas sobre información de destino en la cabecera de la celda, y no sobre el contenido de la carga útil de la celda. Para mover el tráfico a través de la red ATM, los dispositivos en el borde de la red convierten los grupos de tráfico no ATM en celdas. La adición de nuevos tipos de tráfico requiere solamente un dispositivo de borde, ubicado donde existe la demanda de tal tráfico.

ATM es un servicio de transporte *orientado a conexión.* Dentro de solamente los 5 bytes de cabecera, una celda ATM no puede llevar la dirección de destino completa para cada celda. En su lugar utiliza una dirección abreviada, llamada *identificador de canal virtual,* que provee información suficiente para establecer conexión entre 2 estaciones ATM. Una vez que la conexión existe a través de la red ATM, la comunicación está asegurada.

Las LANs tradicionales, por otro lado emplean tecnología de transmisión sin conexión basada en direccionamiento de 48 bits. Así, los dispositivos de borde deben tener alguna forma de adaptarse de los protocolos de la capa de red, tales como IP e IPX, al paradigma de la conmutación orientada a conexión.

Una muy importante interfaz de interoperatibilidad con LANs tradicionales es el LAN *Emulation* User-to-Network Interface (LUNI). Los protocolos LUNI permiten que la red ATM y sus dispositivos de borde controlen las conexiones virtuales requeridas para transmitir y emular la naturaleza sin conexión de una LAN.

C. ATM LAN *Emulation*

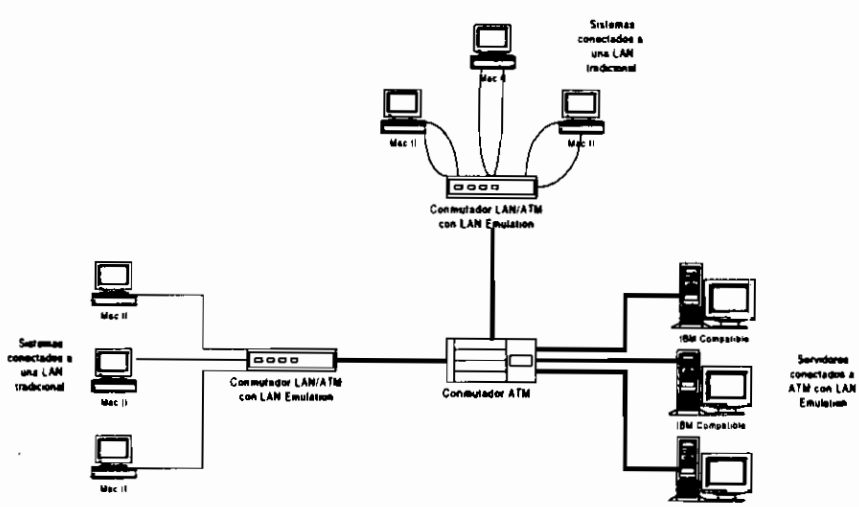


Figura 3.44 Aplicación frecuente de ATM y LAN Emulation

De acuerdo a la versión 1 de la especificación LAN *Emulation* del Forum ATM, "El objetivo principal del servicio LAN *Emulation* es habilitar las aplicaciones existentes para accesar a una red ATM vía el *stack* de protocolos como APPN, NetBIOS, IPX, etc, como si estuviera corriendo sobre una LAN tradicional". LAN *Emulation* es una función de los dispositivos de borde así como una función del sistema terminal ATM

que permite que el protocolo de conectividad de datos de ahora disfrute de conectividad de alta velocidad (ATM) sin modificación. Las tradicionales estaciones terminales pueden utilizar LAN *Emulation* para conectarse a otros sistemas tradicionales, así como a servidores, ruteadores, *hubs* y otras estaciones conectadas a redes ATM.

LAN *Emulation* provee una capa de traducción entre los protocolos de nivel más alto que no están orientados a conexión, y los niveles de protocolo más bajo ATM orientados a conexión.

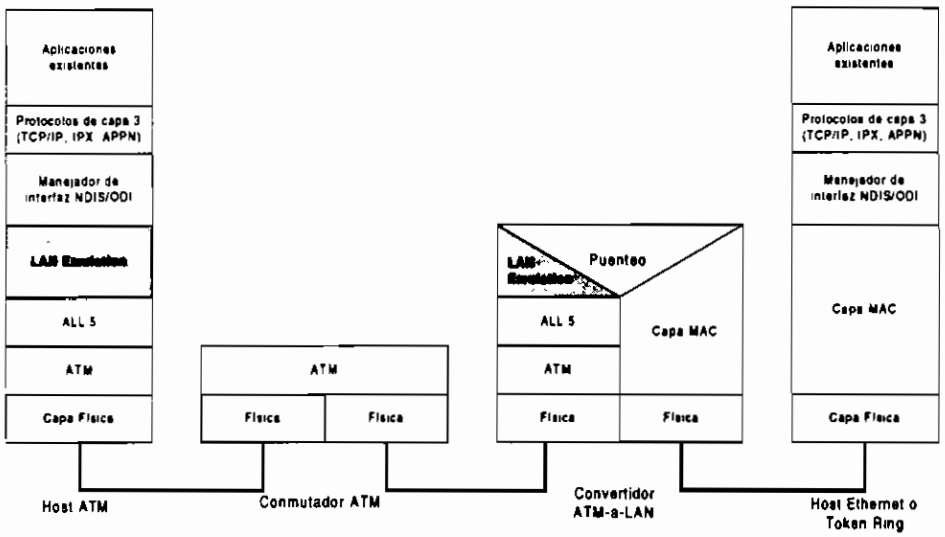


***Figura 3.45* Función de LAN Emulation**

Consideremos las diferencias de la capa de protocolo entre el *host* ATM en el lado izquierdo de la figura 3.45 y el *host Ethernet* o *Token-Ring* en el lado derecho. En el *stack* de protocolos BISDN, la capa ATM se sitúa directamente sobre la capa física. Muchas capas físicas son especificadas, incluyendo algunas para 100 y 155 Mbps. El interfaz WAN de 155 Mbps a la red pública estará basada sobre *Synchronous Optical Network* (SONET), y otros factores de mercado indican que los interfaces basados en SONET predominarán a través de la LAN.

La capa ATM maneja la cabecera para celdas ATM de longitud fija. Aquel acepta la carga útil de la celda de una capa más alta, añade la cabecera, y pasa la celda resultante de 53 bytes a la capa física. Posteriormente, se reciben las celdas de la capa física, se separa su cabecera y pasan los restantes 48 bytes a los protocolos de capas más altos. Para la capa ATM son transparentes los tipos de tráfico que lleva, aunque distingue la calidad de servicio a través de información aprendida durante la configuración de la conexión.

La capa adaptiva de ATM (*ALL-ATM Adaptation Layer*) se sitúa sobre la capa ATM. El AAL formatea los datos dentro de los 48 bytes de carga útil de la celda ATM, conociendo este proceso como segmentación. Una vez que las celdas ATM alcanzan su destino, ellas son reconstruidas en los niveles más altos de datos y transmitidos a los dispositivos locales respectivos en un proceso referido como reensamblaje. Debido a que ATM puede llevar múltiples tipos de tráfico y algunos protocolos

adaptivos, cada operación simultáneamente existe en una capa adaptiva. ALL tipo 5 es utilizada por LAN *Emulation*.

LAN *Emulation* se sitúa sobre ALL 5 en la jerarquía de protocolos. En la conversión ATM a LAN en el borde de la red, LAN *Emulation* soluciona problemas de conectividad de datos para todos los protocolos -ruteables y no ruteables- por puenteo de direcciones LAN a ATM en la capa MAC. LAN *Emulation* es completamente independiente de los protocolos de capas superiores, servicios y aplicaciones.

Debido a que LAN *Emulation* ocurre en dispositivos de borde y sistemas terminales, aquel es enteramente transparente a la red ATM y a los dispositivos terminales (*Ethernet* o *Token-Ring*). LAN *Emulation* enmascara completamente la configuración de conexión y funciones de manejo requeridas por el conmutador ATM de las capas de protocolos más altos. De esta forma, "mapea" las direcciones MAC en conexiones virtuales de ATM, con lo que la red ATM parece funcionar como una LAN no orientada a conexión.

Soporte de múltiples LAN emuladas

El estándar de LAN *Emulation* de ATM ha determinado que debe soportar la existencia de varias o múltiples emulaciones de LAN sobre la misma capa física de ATM.

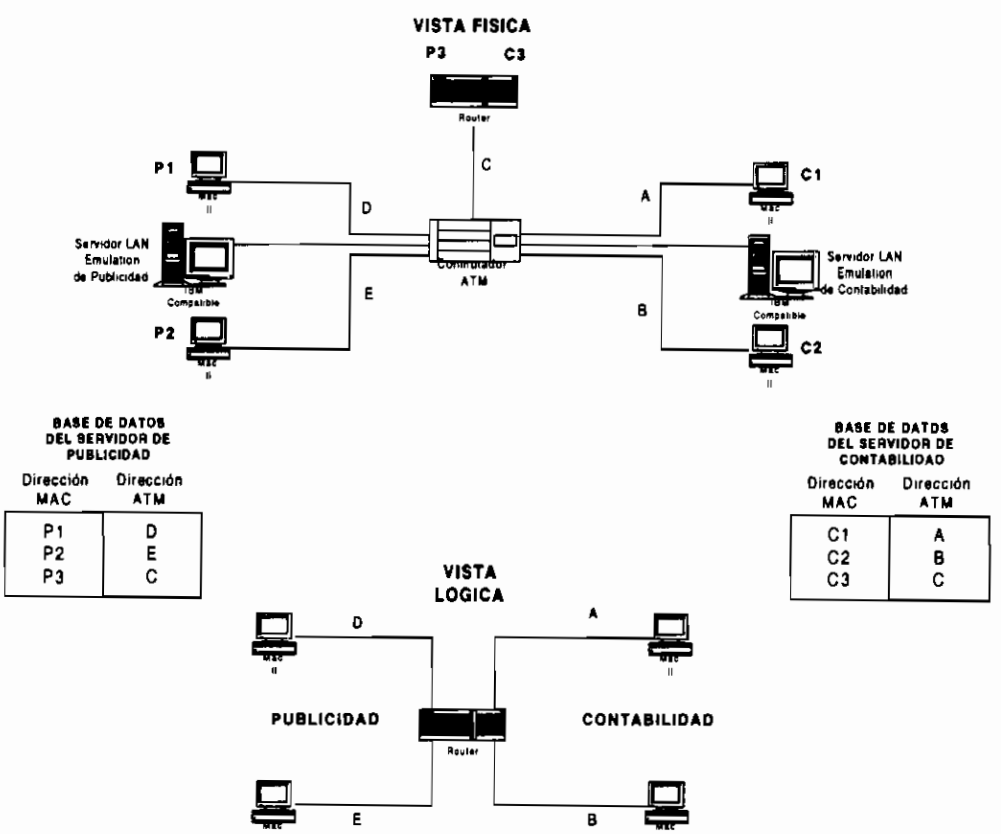


***Figura 3.46** Vistas física y lógica de una red configuradas con conexiones virtuales*

LAN Emulation es implementada bajo el concepto cliente/servidor. Un cliente de *LAN Emulation* resuelve direcciones MAC, administradas por las funciones del servidor *LAN Emulation*. Cada cliente se conecta al servidor con una conexión virtual. Solamente los clientes conectados al mismo servidor pueden conocer sobre los otros que están directamente conectados, y comunicarse con ellos. La segmentación lógica de la red a través de múltiples funciones del servidor, las cuales pueden ser dispositivos solitarios, *software* dentro de sistemas, o módulos de conmutación ATM, permite que varias LAN emuladas coexistan simultáneamente sobre la misma capa física de red.

En la figura 3.46 puede observarse las vistas física y lógica de múltiples LAN emuladas. En la vista física, puede observarse como la LAN de contabilidad está compuesta de dos clientes y un servidor, al igual que el área de publicidad. En la vista lógica puede verse la separación lógica real entre las dos LANs.

Cada servidor departamental guarda la pista de sus clientes en una base de datos residente. Cuando el cliente C1 de contabilidad envía un paquete al cliente C2, éste pasa primero al servidor de contabilidad y el paquete es transmitido luego a C2. Si C1 desea enviar un paquete a P2, el paquete llega primero al servidor contabilidad, el cual verifica que en su base de datos no existe emparejamiento con una dirección ATM de su LAN, direccionando el paquete hacia el ruteador P3/C3. Este último, envía el paquete hacia el servidor LAN *Emulation* de publicidad, el cual compara su base de datos y determina que la dirección MAC P2 le corresponde al cliente ATM E.

Actualmente, pueden encontrarse productos que tienen integrado un conmutador y un ruteador en el mismo dispositivo (realizando una función de servidor de ruta de alta velocidad); de esta manera, bajo el mismo ejemplo anterior, cuando el cliente de contabilidad C1 desee enviar un paquete a P2, la función del servidor de ruta puede proveer suficiente información a C1 de tal forma que pueda conectarse directamente con P2. Debido a que toda la complejidad de la configuración y *software* están guardadas en el ruteador, la complejidad de configuración no se incrementa; y puesto que las decisiones de envío están basadas sobre las direcciones de la capa de red, más control está disponible.

D. Redes virtuales ATM

La habilidad de manejar varias LAN emuladas, permite que se puedan crear algunos dominios de LAN puenteados dentro de una única red ATM. Un dominio consiste de un grupo de usuarios que pueden comunicarse directamente.

Las LANs virtuales crean grupos seguros, promoviendo *firewalls* contra tormentas de *broadcast*, utilizan control de flujo para hacer mejor uso del ancho de banda, y permiten a los administradores de red reconfigurar las redes sin requerir cambios en la infraestructura de transporte ni adquisición de equipo adicional.

3.4 EVALUACION DE LAS ESPECIFICACIONES DEL SUBSISTEMA DE CONECTIVIDAD DE UNA RED ESTRUCTURADA DE DATOS

3.4.1 EVALUANDO UNA TARJETA DE INTERFAZ DE RED

Los siguientes criterios son válidos cuando se trata de evaluar una tarjeta de interfaz de red:

a. La clase de interfaz que conviene a un medio determinado
b. Compatibilidad de protocolos
c. La arquitectura de la interfaz de red que aseguraría cumplir determinados requerimientos
d. El rendimiento que será capaz de proveer
e. La flexibilidad
f. La confiabilidad
g. La facilidad de administración

3.4.1.1 Clase de interfaz que conviene a determinado medio

Dentro de este ítem resulta importante considerar:

- Tipo de conector requerido: en algunos casos puede requerirse un interfaz con 2 tipos de conectores (en *Ethernet* por ejemplo BNC y RJ45)
- Determinados medios donde existen 2 velocidades de transmisión de datos (en *Token-Ring* por ejemplo 4 Mbps o 16 Mbps, o en *Ethernet* 10 ó 100 Mbps)
- Configuración de la interfaz: utilizando *jumpers, dip switches* ó *software*
- Utilización en estaciones de trabajo donde se requiera bajo rendimiento, o utilización en estaciones con alta carga de trabajo y servidores

3.4.1.2 Compatibilidad con protocolos

Es muy importante considerar el *stack* de protocolos y los sistemas operativos para los que las tarjetas ofrecen soporte de *drivers*. Por ejemplo: Netware 3.1x, 4.x, Microsoft LAN Manager, Microsoft Windows NT, Windows 95, etc.

3.4.1.3 Arquitectura de las interfaces de red

Deben considerarse especialmente las siguientes características de arquitectura:

- Compatibilidad de *hardware*: IBM PC AT, computadores compatibles
- Estructura del bus: ISA, EISA, MCA, VESA, PCI

- Modo de transferencia de datos: I/O ,*Bus Master*

A. Estructura del bus de datos

A.1 ISA (Industry Standard Architecture)

El bus ISA es un bus de 16 bits que puede transmitir datos de 8, 16 o 32 bits. Debe considerarse que ISA es un cuello de botella para sistemas operativos de 32 bits, pues tiene que dividir los datos en paquetes de 16. Además, ISA no aprovecha las capacidades de procesamiento de los procesadores de 32 bits (80386, 80486, pentium).

A.2 EISA (Extended Industry Standard Architecture)

EISA es una arquitectura de bus de 32 bits, posee compatibilidad hacia atrás (con los buses ISA) y tiene características de autoconfiguración. A pesar de existir compatibilidad con las tarjetas ISA, no es conveniente insertar una tarjeta ISA en un bus EISA cuando se tiene un arreglo con tarjetas EISA, ya que posiblemente se reduzca el rendimiento del arreglo. En resumen, la arquitectura EISA posee las siguientes características generales:

- Direccionamiento de memoria de 32 bits
- Transferencia de datos de 8/16 o 32 bits
- Velocidades de transferencia de 33 MB/s y 8.33 MHz
- Soporte para tarjetas *Bus Master*, DMA mejorada por interrupciones compartidas
- Configuración automática por *software*

A.3 MCA (Micro Channel Architecture)

No tienen compatibilidad con ningún otro tipo de arquitectura y pueden ser de 16 o 32 bits.

A.4 Bus VL

El estándar bus VL, está basada en una arquitectura de *bus local*, y lo mantiene *Video Electronics Standards Association* (VESA).

La arquitectura de bus local, utiliza toda la velocidad de los procesadores más modernos. Supongamos un computador con procesador 486 DX2 que posee una arquitectura de 32 bits y funciona a 66 MHz. Su potencia podría verse limitada por un bus ISA tradicional de 8 ó 16 bits que funciona a 8 MHz. El bus EISA proporciona un "vía" más amplia, de 32 bits, pero el "límite de velocidad" sigue siendo 8 MHz. El bus local, proporciona la misma vía de 32 bits, pero aumenta el límite de velocidad a una velocidad de reloj teórica igual a la del procesador: 66 MHz.

El estándar provista por VESA soporta hasta 2 dispositivos en un bus VL.

A.5 PCI (*Peripherical Component Interconnect*)

También está basada en una arquitectura de bus local, con direccionamiento de 32 bits, reconocimiento automático de tarjetas, capacidad de *plug and play*, trabajando a la velocidad del bus del procesador. PCI soporta hasta 10 dispositivos en un bus, con dos buses hasta 20 dispositivos. Por estas razones PCI ha sido de mayor aceptación que la arquitectura sostenida por VESA.

B. Modo de transferencia de datos

B.1 Control con puertos I/O (*Input Output*)

En este modo de transferencia, cada uno de los dispositivos añadidos solicita al procesador principal atienda sus requerimientos mediante una interrupción, y tiene en cuenta el pórtico de entrada/salida (I/O) que le corresponde a cada dispositivo.

B.2 *Bus Master*

Es una característica que poseen los dispositivos de expansión (tarjetas de red por ejemplo), que poseen un procesador propio para controlar su flujo de datos con la memoria y con otros dispositivos de expansión que también sean *Bus Master*, sin tener que pedir autorización al procesador principal. Esto permite mejorar el rendimiento de la tarjeta de red y otros dispositivos de expansión, y liberar la carga de trabajo de procesador principal.

3.4.1.4 Rendimiento

- El rendimiento de una tarjeta de red debe medirse principalmente por sus características de estructura en el bus de datos y por su modo de transferencia de datos. Tarjetas de red de arquitectura idéntica, pero de diferentes proveedores podrían proveer diferente rendimiento, debido a características de compatibilidad con el equipo sobre el cual funciona y el sistema operativo instalado en aquel. En este sentido, el rendimiento también se vería afectado por el tiempo de funcionamiento útil de la tarjeta, ya que si bien en momentos de funcionamiento óptimo, dos tarjetas de proveedores diferentes pueden dar el mismo rendimiento, cuando se hace una medición en tiempos de funcionamiento prolongados, el número de caídas de las tarjetas definiría su rendimiento real. Por tanto, es conveniente que antes de elegir la interfaz de red sólo por sus características de arquitectura, también se revisen antecedentes de compatibilidad.

3.4.1.5 Flexibilidad

La flexibilidad de una interfaz de red, se mide principalmente por su capacidad de adecuarse a la mayor parte de medios, velocidades, sistemas

operativos y protocolos. Se mide además por su facilidad de configuración, especialmente características de autoconfiguración (*plug and play*) y configuración por *software* (no con *jumpers o dip switches*).

3.4.1.6 Confiabilidad

Cuando se considera confiabilidad, es importante considerar el tiempo máximo de funcionamiento, garantía, servicio y soporte, lo que fundamentalmente está en función del fabricante.

3.4.1.7 Facilidad de administración

La administración de las interfaces de red, debe verificarse principalmente en la existencia de soporte de un agente de administración (SNMP por ejemplo). Una interfaz administrable, permitirá que se realicen verificaciones remotas de su funcionamiento, características e inventario.

3.4.2 EVALUANDO UN *HUB*

Debido principalmente a que los *hubs*, son básicamente concentradores que realizan funciones relativamente sencillas asociadas con la capa física del modelo de referencia OSI, éstos no realizarán operaciones ni de puenteo, conmutación o ruteo. Los siguientes criterios son válidos cuando se trata de evaluar un *hub*:

a. El tipo de *hub* que conviene a un medio determinado
b. Compatibilidad de protocolos
c. La arquitectura del *hub* que aseguraría cumplir determinados requerimientos
d. El rendimiento que será capaz de proveer
e. La flexibilidad
f. La confiabilidad
g. La facilidad de administración

3.4.2.1 Tipo de *hub* que conviene a determinado medio

Los *hubs* deben elegirse en concordancia con el medio al cual están asociados, dependiendo de la topología física y lógica que se haya elegido utilizar. Así, por ejemplo, en un ambiente *Token-Ring* con cable STP son utilizados *hubs* generalmente de 8 puertos, mas conocidos como MAUs. Son especificaciones importantes del medio las siguientes: tipo de conector, número máximo de pórticos por *hub*, número máximo de *hubs* por *stack* o pila, opciones de actualización y de dispositivos redundantes para tolerancia a fallas.

Es importante, también determinar el tipo de *hub* que conviene según la ubicación física de los mismos, pues a pesar de que la recomendación actual (de cableado estructurado), aconseja tener los elementos activos concentrados, podrían presentarse situaciones en las que esto no es posible, y debería entonces considerarse la posibilidad de adquirir *hubs* que permitan configuración distribuida. Actualmente, la mayoría de fabricantes ofrecen las dos posibilidades, es decir se permite configuración de *hubs* apilados para ambientes concentrados (normalmente a través de un conector de apilación especial con mayor ancho de banda que el de los pórticos del *hub*) ó se permite también configurar *hubs* distribuidos mediante la conexión de pórticos del mismo *hub* o conectores especiales para este efecto.

La desventaja de no poseer conectores especiales para apilación o conexión en *backbone*, es principalmente que el ancho de banda utilizado para comunicación entre dos *hubs* apilados o conectados en un ambiente distribuido, resulta pequeño, originando un "cuello de botella" en ese punto. Para disminuir este efecto, existen también *hubs* en chasis que permiten un crecimiento modular. Cada vez que más pórticos sean requeridos, puede añadirse un módulo más al chasis, permitiendo en algunos casos incluso la mezcla de varias topologías con funciones de puenteo localizados en otro módulo. La ventaja del crecimiento modular en un mismo chasis, es principalmente el compartir el mismo bus de datos, lo que no limita el ancho de banda de comunicación entre grupos de pórticos de *hubs* (módulos) diferentes.

3.4.2.2 Compatibilidad con protocolos

Es muy importante considerar los *stack* de protocolos y tramas para los cuales los *hubs* tienen soporte. Esto normalmente puede encontrarse en las especificaciones de soporte de protocolos que vienen en los manuales.

3.4.2.3 Arquitectura de *hubs*

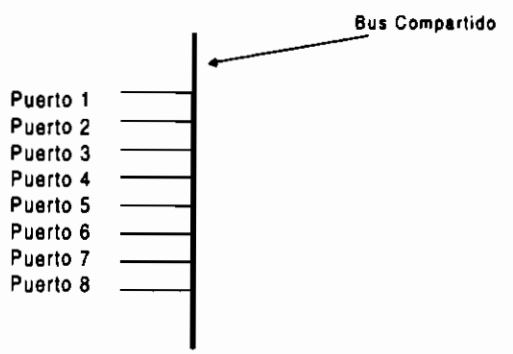


***Figura 3.47** Esquema de conexión de pórticos al bus de un hub de acceso compartido*

En general, los *hubs* comparten un canal común para todos los pórticos conectados. Es decir poseen un ancho de banda compartido entre los pórticos que se encuentran conectados al *hub*, tal como se muestra en la figura 3.47.

Cuando se quiere aumentar el número de pórticos disponibles para un área de trabajo, esto se consigue mediante la conexión de otro *hub* al primero, y así sucesivamente. La conexión puede conseguirse utilizando un pórtico por cada uno de los *hubs*, o mediante un conector especial de apilamiento que posee un ancho de banda mayor que el que permite el de conexión directa a través de pórticos.

Los distintos tipos de *hubs*, fundamentalmente se diferencian en su arquitectura:

- **Hubs multiservicio basados en chasis**: En este tipo de *hubs*, el aumento de pórticos se consigue mediante el aumento de módulos al chasis original, el cual pudo haber venido con pórticos deshabilitados. La ventaja de este tipo de *hubs* es que su arquitectura presenta un bus común con un amplio ancho de banda para la comunicación entre los diferentes módulos, reduciendo la posibilidad de que se generen cuellos de botella entre grupos de pórticos.

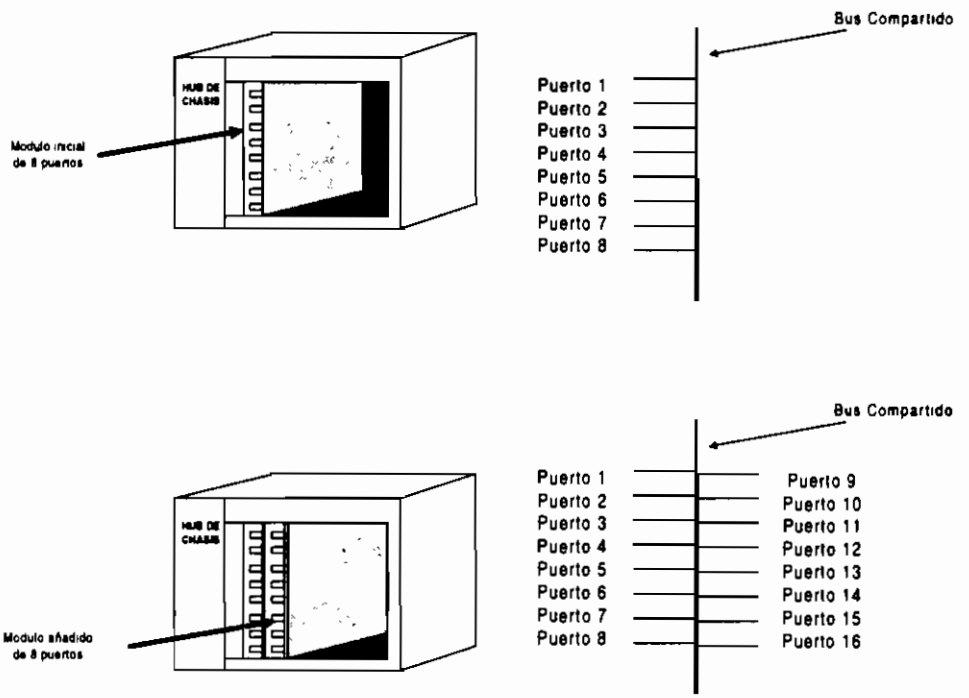


***Figura 3.48** Esquema de conexión de pórticos al bus de un hub modular de acceso compartido*

- **Hubs apilables**: En este tipo de *hubs*, el aumento de pórticos se consigue mediante el aumento de *hubs*, interconectados mediante cables especiales de apilamiento, que proporcionan un mayor ancho de banda para su

interconexión. Generalmente estos *hubs* deben ir apilados, pues estos cables de apilamiento no soportan distancias largas.

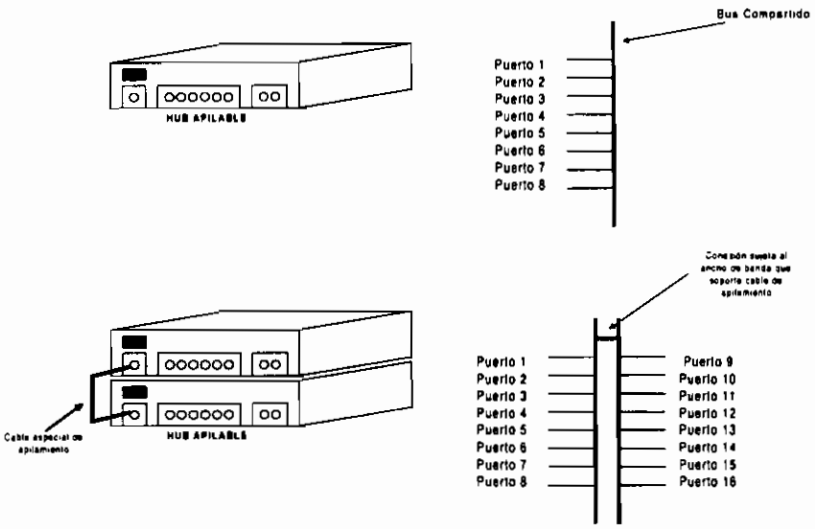


***Figura 3.49** Esquema de conexión de pórticos a los buses de 2 hubs de acceso compartido apilados*

- **Hubs de unión por pórtico**: Este tipo de *hubs*, se conecta con otros *hubs* mediante el sacrificio de uno de sus pórticos, para aumentar el número de pórticos disponibles a la red. A pesar de tener la ventaja de poder colocarlos distribuidos (lo cual puede ser útil en algunas circunstancias, aunque administrativamente no) su gran desventaja es que el ancho de banda disponible para la conexión entre *hubs*, es el mismo que está disponible a cada uno de los pórticos, generando comúnmente "cuellos de botella" en el tráfico de datos entre *hubs*.

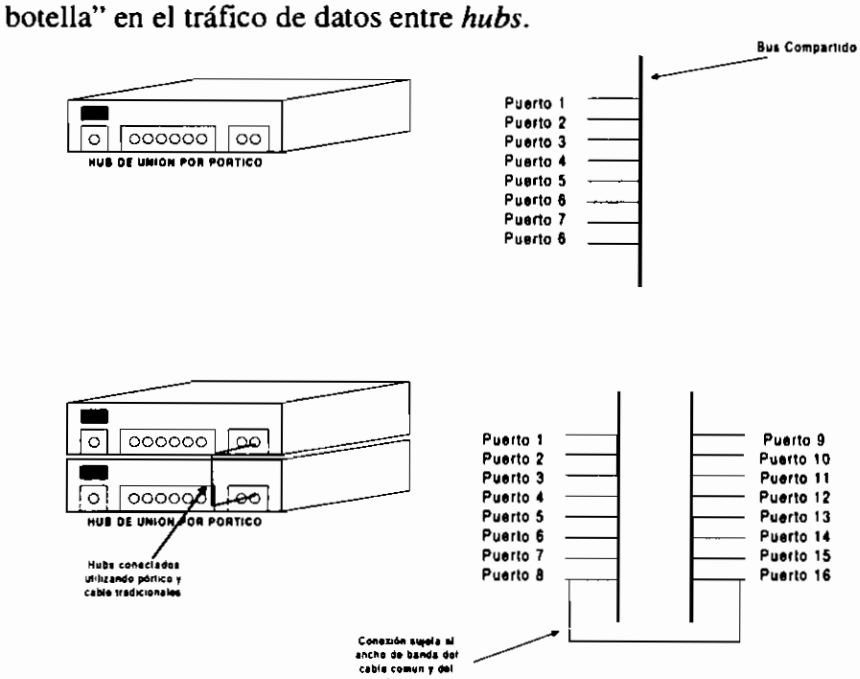


***Figura 3.50** Esquema de conexión de pórticos al bus de 2 hubs de acceso compartido conectados a través de pórticos de estación*

d. Rendimiento

El rendimiento de los *hubs*, se ve mejorado con la implementación de módulos de puenteo, que permiten hacer segmentaciones y localizar el tráfico hacia el servidor, mejorando el rendimiento de la red.

3.4.2.4 Flexibilidad

Fundamentalmente orientada al tipo de conectores que soporte y a la facilidad de funcionamiento con otros dispositivos (compatibilidad) tales como ruteadores, conmutadores y puentes. Soporte a velocidades de transmisión de datos por ejemplo 4 y 16 Mbps para *Token-Ring*, o 10 y 100 Mbps para *Fast Ethernet*. Soporte para opciones con módulos de administración SNMP o RMON[35]. Soporte a módulos para funciones de *bridge*.

3.4.2.5 Confiabilidad

Esta característica debe medirse fundamentalmente por la robustez del diseño para asegurar la mayor cantidad de tiempo en funcionamiento. Deben ser soportadas características de tolerancia a fallas y características de redundancia (fuentes redundantes por ejemplo).

3.4.2.6 Administración

Deben medirse características de facilidad de administración tales como: administración vía TELNET, un módem, consola de administración local o SNMP que incluya MIB, MIB I y MIB II o RMON.

3.4.3 EVALUANDO UN PUENTE

Para determinar los requerimientos que debe cumplir un puente LAN, deben evaluarse los siguientes criterios:

a. La clase de puente que conviene a un medio determinado
b. La arquitectura del puente que aseguraría cumplir determinados requerimientos
c. El rendimiento que será capaz de proveer
d. La flexibilidad
e. La confiabilidad

[35] SNMP, RMON y MIB son protocolos para administración de redes que serán explicados en el numeral 3.5.

f. La facilidad de administración

3.4.3.1 Tipos de puentes

Los puentes son dispositivos que se utilizaron y difundieron ampliamente, especialmente durante el desarrollo de redes *Token-Ring*, *Ethernet* y FDDI. En la actualidad son más utilizados los ruteadores y *switches* ya que realizan funciones más completas, especialmente en aplicaciones donde se requiere comunicar varias LANs en un punto de convergencia. Adicionalmente, las tecnologías basadas en ruteadores y conmutadores se han convertido en tecnologías robustas a precios más aceptables. Sin embargo, cuando se habla de grupos de trabajo pequeños, aún son aplicables los puentes.

A. Puentes transparentes

Son utilizados para conexión de redes LAN a LAN en las que las arquitecturas de enlace de datos son iguales, bien sean sólo *Ethernet* o sólo *Token-Ring*. Son aplicables en ambientes donde el tráfico de envío de *broadcast* y *multicast* no son críticos.

B. Puentes de árbol de cruce transparente

Son muy útiles cuando las redes crecen y comienzan a ser más complejas, y la posibilidad de crear múltiples caminos o lazos entre las LANs se incrementa. Los lazos pueden causar estragos a una red basada solamente en puenteo transparente y además la duplicación de paquetes y *broadcast*, degradan el rendimiento de la red.

Para combatir el problema de lazo activo, el algoritmo de puenteo conocido como *Spanning tree Algorithm (STA)* fue desarrollado proveyendo la siguiente funcionabilidad:

- Configura una topología activa predecible de LANs puenteadas dentro de un único árbol de puentes tal que haya sólo un camino lógico entre cualesquiera dos segmentos de LAN; eliminando así cualquier posibilidad de lazos en la red.
- Provee un camino tolerante a fallas utilizando reconfiguración automática de la topología del árbol de puentes como un resultado de falla en un puente o por desperfecto en el camino de datos.
- Consume una cantidad mínima de ancho de banda para establecer y mantener un camino del árbol de puentes.
- Su operación es transparente a los nodos finales

Por estas características son útiles en ambientes donde es importante tener siempre disponible un camino de comunicación que sea tolerante a fallas. Son diseñados principalmente para conexión entre redes *Ethernet*.

C. Puente de enrutamiento de fuente

Por sus características de "enrutamiento básico", genera menor tráfico de *multicast* y *broadcast* con selección de caminos, siendo utilizados para conectar redes *Token-Ring* con un máximo de 7 saltos entre ellas.

D. Puentes de enrutamiento de fuente transparente

Debido a que son una combinación de un puente de enrutamiento de fuente con un puente transparente, proveen conexión entre redes LAN que tienen arquitecturas de enlace de datos de enrutamiento de fuente y de no enrutamiento de fuente. Son usadas para conexiones de red LAN a LAN, locales o remotas, principalmente *Token-Ring*, ya que se basan en el algoritmo de fuente de ruta. Son susceptibles[36] a tráfico por *multicast* y *broadcast*.

E. Puentes de encapsulamiento

Un puente de encapsulamiento es generalmente asociado con topología *backbone* tales como conexiones IEEE 802.3 y 802.5 a FDDI. Debe tenerse claro que este tipo de puentes solo encapsula la capa de enlace de datos de una LAN dentro de la capa de enlace de datos de la otra, es decir no permite la comunicación directa entre diferentes tipos de LAN. De este modo, si se quisiera comunicar una LAN *Ethernet* a una *Token-Ring* utilizando este tipo de puentes, sería necesario una topología adicional, tal como FDDI por ejemplo, y dos puentes: el uno que encapsule de *Ethernet* a FDDI y el otro que trabaje entre FDDI y *Token-Ring*. Adicionalmente son susceptibles al tráfico de *broadcast* y *multicast*.

F. Puente translacional

Este tipo de puente es una forma especial de puente transparente que permite la conexión entre LANs que tienen diferentes arquitecturas de la capa de enlace de datos y física, por ejemplo, permite la conexión entre una LAN *Ethernet* y *Token-Ring*. Es independiente del protocolo de la capa de red, pero depende de la capa de enlace de datos. Es susceptible al tráfico de *multicast* y *broadcast*. Debido a que su funcionamiento se basa en la manipulación de la envoltura de la trama, el procesamiento es relativamente directo debido a que la envoltura de las redes *token*, *Ethernet* y FDDI son semejantes.

3.4.3.2 Arquitectura del puente

La arquitectura de un puente es relativamente más compleja de evaluar ya que fundamentalmente se conoce una sola tecnología basada en tres unidades sobre cada puerto: unidad de servicio MAC, unidad de MAC Relay y la

[36] El término susceptibles se refiere a que pueden ser afectados negativamente.

unidad de protocolo del puente. Cada una de estas unidades y fue analizada en el numeral 3.2.2.3 de este capítulo.

3.4.3.3 Rendimiento

Uno de los factores que determinan de manera más crítica el rendimiento de un puente es el tiempo que se toma el puente en el proceso de envío. Para este proceso, se provee de almacenamiento para las tramas en espera, guardando por lo general un esquema de orden FIFO que es mantenido por los puentes de la capa MAC. Considerando que las tramas podrían ser removidas de la cola de envío, ya sea porque se ha excedido el tiempo de almacenamiento en memoria, demora en la transmisión o porque el puerto asociado dejó de estar en estado de envío, una característica que definirá el rendimiento en el proceso de envío, será la cantidad de *buffers* que tiene disponible el puente para almacenar tramas en la cola de envío, garantizando de esta forma el menor número de retransmisiones en cada uno de los segmentos. Debe considerarse que el rendimiento del puente afectará el rendimiento de cada uno de sus segmentos, por lo que es conveniente elegir el tipo puente que le conviene al medio.

3.4.3.4 Flexibilidad

Considerando los principales tipos clasificados según la aplicación a la cual son útiles, es importante recordar que se han fabricado modelos de puentes, que permiten todas las configuraciones en un solo dispositivo, cada una de las cuales pueden ser elegidas mediante administración por *software*.

Adicionalmente, se pueden encontrar en el mercado, dispositivos modulares que permiten configuraciones de concentradores (*hubs*) y puentes a la vez.

3.4.3.5 Confiabilidad

Esta característica debe medirse fundamentalmente por la robustez del diseño para asegurar la mayor cantidad de tiempo en funcionamiento. Deben ser soportadas características de tolerancia a fallas y características de redundancia (fuentes redundantes por ejemplo).

3.4.3.6 Administración

Deben medirse características de facilidad de administración en banda y fuera de banda, tales como: administración vía TELNET, módem, consola de administración local o SNMP que incluya MIB, MIB I y MIB II o RMON.

3.4.4 EVALUANDO UN CONMUTADOR

Para determinar los requerimientos que debe cumplir un conmutador LAN, deben evaluarse los siguientes criterios:

a. La clase de conmutador que conviene a un medio determinado
b. El método de envío de paquetes utilizado
c. La arquitectura del conmutador que aseguraría cumplir determinados requerimientos
d. El rendimiento que será capaz de proveer
e. La flexibilidad
f. La confiabilidad
g. La facilidad de administración

3.4.4.1 Clases de conmutadores LAN

Los conmutadores LAN se han clasificado generalmente en las siguientes clases:

1. Conmutador de Nodo/Grupo de trabajo (*Node /workgroup*)
2. Conmutador de segmento
3. Conmutador de *backbone*

A. Conmutador de Nodo/Grupo de trabajo

Este tipo de conmutador intenta proveer un ancho de banda y velocidad incrementados para un único grupo de trabajo (generalmente con un pequeño número de nodos). Estos grupos de trabajo por lo general solamente tienen un servidor y cada cliente podría tener una conexión directa al conmutador.

B. Conmutador de segmento

Estos conmutadores tratan de conectar conmutadores de grupo de trabajo y/o *hubs* compartidos. Estos conmutadores tienen tablas de direcciones más grandes, y son más flexibles en sus configuraciones de puertos, soportando además salidas con velocidades más altas.

C. Conmutador de *backbone*

Estos conmutadores son diseñados para interconectar un sitio muy grande, y proveer conectividad a servicios remotos. El conmutador de *backbone* debe ser ampliamente modular y proveer conexiones de alta

velocidad (ATM, FDDI, por ejemplo). Generalmente ellos tienen opciones para servicios de enrutamiento *built-in*[37].

3.4.4.2 Métodos de envío de paquetes

Como se había mencionado anteriormente, existen fundamentalmente dos métodos de envío de paquetes:

1. Almacenamiento y envío (*Store and forward*)
2. Salida directa (*Cut through*)

A. Método de almacenamiento y envío

El método de almacenamiento y envío almacena los paquetes de datos en orden dentro de *buffers* para realizar una verificación completa de errores y filtración, para posteriormente enviar los paquetes fuera del conmutador.

Este método es generalmente utilizado cuando se requiere mover tramas desde una LAN de baja velocidad (10 Mbps por ejemplo) a una LAN de alta velocidad (100 Mbps por ejemplo). Este método está incrementalmente siendo utilizado para verificación de errores y para envío de datos en ambientes de velocidad dual (10/100 Mbps por ejemplo).

En este método la latencia se mide como el tiempo transcurrido entre el último bit recibido y el primer bit transmitido (LIFO). Esto no incluye el tiempo que le toma recibir el paquete entero, el cual puede variar de acuerdo al tamaño del paquete, desde 65 microsegundos hasta 1.3 milisegundos aproximadamente.

B. Método de salida directa (*cut through*)

El método más tradicional salida directa *(cut-through)* envía inmediatamente el paquete fuera del conmutador para disminuir la *latencia* (la cantidad de tiempo que le toma al conmutador en procesar un paquete), pero sin realizar una verificación de errores dentro del conmutador. Debido a que el envío arranca antes de que el paquete entero sea recibido, podrían haber ocasiones en las que los paquetes son enviados con errores.

En este método la latencia se mide como el tiempo transcurrido entre el primer bit recibido y el primer bit transmitido (FIFO).

[37] Los servicios de enrutamiento dentro de un mismo *switch* (conmutador) utilizan funciones de la capa red, por lo que a este tipo de conmutadores se los conoce generalmente como *conmutadores inteligentes (o smartswitches).*

C. Otros métodos

Dos variaciones que generalmente son clasificadas dentro de *cut through* son *fast forward* y *fragmentfree*, sin embargo estos métodos de envío de paquetes están basados en la combinación de los dos métodos: *store and forward* y *cut through*.

C.1 Fast Forward

Este método reduce significativamente la latencia por decisiones de procesamiento de envío mientras el paquete está siendo almacenado. En este método se entrega rendimiento *cut through* con una confiabilidad *store and forward*. Debido a que podrían hacerse envíos con errores, y debido a que el adaptador de red podría requerir de reenvío, un sobreflujo de tráfico podría generarse volviéndose inaceptable en ciertos ambientes. En *fastforward*, la latencia es medida como el tiempo transcurrido entre el primer bit recibido y el primer bit transmitido (FIFO).

C.2 Fragmentfree

En este método, el conmutador filtra los fragmentos que se suponen con colisión, que son la mayoría de los paquetes con error, antes de ser enviados. En una red funcionando apropiadamente, los fragmentos colisionados deben tener un tamaño menor a 64 bytes. Cualquier paquete mayor que 64 bytes es considerado un paquete válido y usualmente es recibido sin error. En los conmutadores que utilizan *fragmentfree* esperan hasta que el paquete recibido haya sido determinado como libre de colisión antes de ser enviado. En este modo, la latencia es medida como FIFO.

3.4.4.3 Arquitectura de conmutadores

Los conmutadores pueden ser de diseño ASIC o basados en procesador.

Los conmutadores basados en procesador son construidos con procesadores de industria estándar, estando el conmutador hecho con *software*. Los conmutadores que utilizan ASIC son una combinación de *hardware* y *firmware* con procesos de conmutación enteramente encapsulados dentro de ASIC. Estos conmutadores son preferibles a los basados en procesador debido a que son mucho más rápidos.

A. *Backplane* compartido

Idealmente, los conmutadores podrían implementar una arquitectura pura de matriz de punto cruzado. Una matriz es básicamente un único ASIC que enlaza múltiples caminos de comunicación con cada uno de los puertos, teniendo un camino dedicado a cada uno de los otros puertos.

En la figura 3.51, cada uno de los pórticos (del 1 al 8) tiene un camino dedicado hacia cada uno de los otros pórticos. Así por ejemplo, si el pórtico 1 requiere enviar paquetes a cualquiera de los otros pórticos, los enviará siguiendo cualquiera de las rutas trazadas con línea punteada, dependiendo del pórtico con el que quiera comunicarse. De la misma forma lo hará el pórtico 2 con los pórticos restantes siguiendo cualquiera de las rutas trazadas con línea delgada continua. De forma análoga lo harán el resto de pórticos.

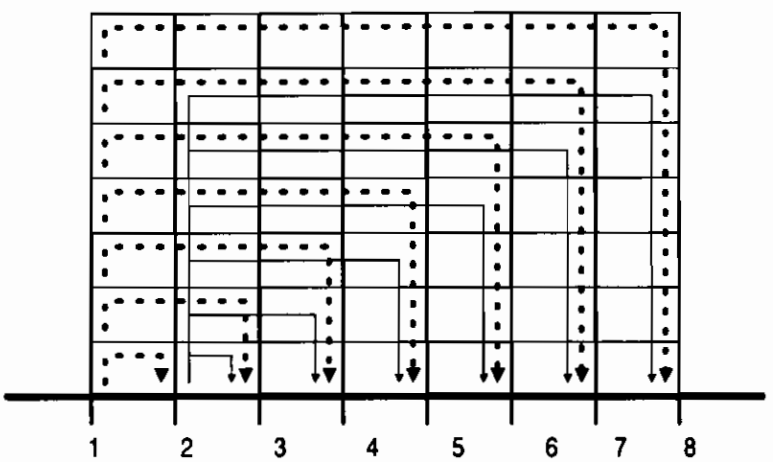


***Figura 3.51** Esquema de conexión de pórticos al bus de un conmutador con backplane matricial*

Desgraciadamente, la arquitectura de matriz pura, no permite expandibilidad, flexibilidad o tecnología de conmutación de cruce (por ejemplo, 10BaseT a 100BaseT). Una matriz pura de punto de cruce también requiere de mucha circuitería.

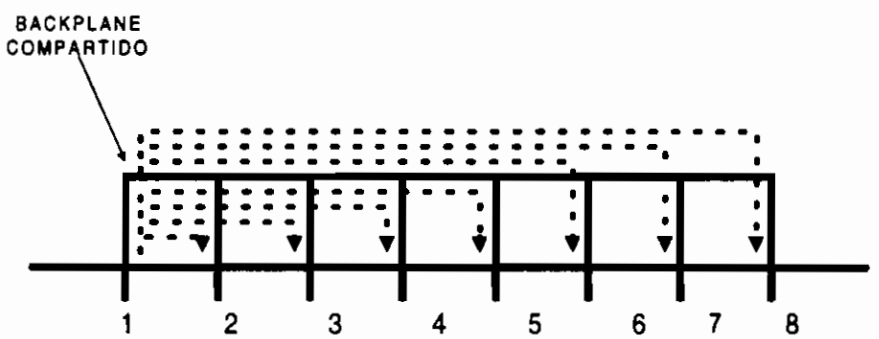


***Figura 3.52** Esquema de conexión de pórticos al bus de un conmutador con backplane compartido*

Algunos laboratorios han sido capaces de retener algunas bondades de la arquitectura de matriz de punto, y sobreponer sus inconvenientes con una arquitectura *backplane* compartido de alta velocidad (ver figura 3.52). Con esta arquitectura, el conmutador comparte su *backplane* con todos los dominios conectados a él. Al contrario de la arquitectura de matriz pura, hay

un camino de datos compartido para cada uno de los puntos. El *backplane* compartido es lo suficientemente rápido para procesar todos los requerimientos de datos, haciendo certeza que no haya contención sobre los segmentos conectados. En las tecnologías de *backplane* compartido, los *backplanes* de alta velocidad pueden manejar fácilmente múltiples conversaciones simultáneas.

B. Implementación de LAN virtuales (VLANs)

Las VLANs se configuran considerando grupos de usuarios que son definidos basados en sus funciones lógicas antes que en su localización física. El criterio para una membresía de VLAN debería ser que el usuario utilice un protocolo común, o ser parte de una misma función departamental. Al contrario de donde los usuarios estén físicamente localizados, los grupos de trabajo pueden ser definidos por su función lógica por medio de simple configuración de un puerto. Las VLANs ofrecen flexibilidad, rendimiento y filtración incrementados. Los usuarios de red asignados a una VLAN son considerados un dominio broadcast separado de tal forma que los paquetes son enviados solamente entre pórticos asignados para la misma VLAN. Con VLANs, el tráfico de *broadcast* en el dominio de cruce, es minimizado y se ahorra ancho de banda al no permitir que los paquetes inunden las salidas de la red. Una VLAN restringe el tráfico *broadcast* a un dominio dado. Ellos crean barreras entre dominios agrupando puertos juntos en VLANs separadas. Estas barreras en los caminos de comunicación ayudan a proveer seguridad entre los dominios. Los mecanismos de seguridad pueden ser fortalecidos entre VLANs separadas.

C. Truncamiento de puerto (Port trunking)

El truncamiento de puerto es utilizado para permitir que algunos puertos puedan conectarse juntos y sean tratados como uno solo, pero como de alta velocidad. Por ejemplo, con truncamiento de puerto, se puede enlazar dos conmutadores juntos con dos puertos de 100 Mbps. De esta forma se conseguiría doblar el rendimiento conmutador-a-conmutador comparado con el conectado con un único pórtico de 100 Mbps.

3.4.4.4 Evaluando el rendimiento de un conmutador

El criterio de rendimiento cuando se evalúan conmutadores es relativa a la velocidad y eficiencia con las cuales un conmutador entrega los datos. Las medidas de rendimiento incluyen: latencia, *throughput*, y su habilidad para ocuparse de la congestión.

A. Latencia

Como se mencionó anteriormente, la latencia es el tiempo que le toma al conmutador procesar un paquete. Es la cantidad de tiempo entre cuando un conmutador recibe una unidad de datos y cuando esa unidad es enviada fuera

del conmutador. La latencia es medida diferentemente dependiendo del método de envío de paquetes utilizado por el conmutador (almacenamiento y envío o *cut through*). La latencia para un dispositivo que utiliza almacenamiento y envío es medida utilizando la lógica LIFO, mientras que para *cut through* se utiliza la lógica FIFO.

LIFO (*last input first output*) significa que la longitud de tiempo considerada es desde el último (*last*) bit de la trama en entrar en un puerto, hasta el primer (*first*) bit que es enviado fuera del puerto de destino. Son comunes encontrar tiempos de latencia que se acercan a los 8 microsegundos (para dispositivos de 10 Mbps) y 3 microsegundos (para dispositivos de 100 Mbps) en conmutadores que utilizan almacenamiento y envío.

FIFO (*first input first output*) significa que la longitud del tiempo considerado arranca desde el momento en que se recibe el primer bit entrante de la trama hasta el momento en que el primer bit es enviado fuera del puerto de destino. Es común encontrar tiempos de latencia en conmutadores que utilizan *cut through* que varían entre 30 y 60 microsegundos (para dispositivos de baja velocidad -10 Mbps-) y tiempos de latencia en conmutadores que utilizan almacenamiento y envío entre 7 y 10 microsegundos (en dispositivos de alta velocidad -100Mbps-). Es importante recordar que los mencionados tiempos de latencia son medidos de formas diferentes (el uno con LIFO y el otro con FIFO) por lo que las comparaciones deben realizarse solo entre dispositivos *cut through* o solo entre dispositivos de almacenamiento y envío.

LATENCIAS APROXIMADAS EN CONMUTADORES DEL MERCADO				
Modo de conmutación	10 Mbps a 10 Mbps	10 Mbps a 100 Mbps	100 Mbps a 100 Mbps	100 Mbps a 10 Mbps
Fast forward (FIFO)	31 microseg.	Na	7 microseg.	7 microseg.
Fragmentfree (FIFO)	70 microseg.	Na	9 microseg.	10 microseg.
Store and forward (LIFO)	7 microseg.	7 microseg.	3 microseg.	3 microseg.

Tabla 3.10 Latencias aproximadas de conmutadores 10/100 Mbps en el mercado

B. Troughput/Tasa de pérdida de paquetes

Throughput es la tasa de transferencia de datos que el conmutador puede sostener sin pérdida de paquetes. Mientras la latencia mide la demora de una única trama, el throughput mide el número de paquetes, o tramas por segundo sin pérdida de paquetes. En un conmutador, el throughput es típicamente

medido en paquetes por segundo (pps), pero también podrían ser referidos como tramas por segundo.

La tasa de pérdida de paquetes es el porcentaje de paquetes que el conmutador no envía dentro de una ventana de tiempo cuando los datos le fueron enviados. Un paquete es definido "perdido" en este caso, si no se ha enviado dentro de cierto período de tiempo.

Para evaluar el número de paquetes por segundo (pps) entre diferentes conmutadores, deben observarse el número de pórticos de conmutación, y la velocidad del medio de los puertos que son conmutados.

C. Control de congestión

La congestión ocurre en el momento en que un número de paquetes son enviados a un segmento en particular, cuya capacidad es superada por ese número. Los datos son entonces retenidos en los *buffers* de memoria hasta que puedan ser enviados a su destino. Si no existiera suficiente memoria, por razones de congestión u otras, los paquetes serán dados de baja. Algunos conmutadores intentan manejar la congestión, haciendo que un segmento que está siendo usado pesadamente, parezca tener numerosas colisiones, causando que todas las estaciones sobre ese segmento suspendan el envío de paquetes. Este método es llamado *backpressure*. Con este método, todos los nodos sobre un segmento son prevenidos de transmitir durante el tiempo en que el conmutador está aplicando *backpressure*, y el tráfico no destinado para el conmutador también es detenido durante este tiempo.

3.4.4.5 Evaluando la flexibilidad de un conmutador

Un conmutador de alto rendimiento debe proveer conexiones de altas velocidades para servidores de archivos y *backbones*, y conexiones de baja velocidad para estaciones y dispositivos de red.

3.4.4.6 Evaluando la confiabilidad de un conmutador

Cuando se considera confiabilidad, es importante considerar el tiempo de funcionamiento máximo seguro, garantía, servicio y soporte.

A. Tiempo de funcionamiento máximo seguro

Un conmutador puede ser usado con una fuente de poder redundante para asegurar la mayor cantidad de tiempo en servicio. Además pueden obtenerse conmutadores que posean módulos intercambiables en caliente, es decir se pueden cambiar módulos del conmutador mientras se encuentra funcionando, sin necesidad de detener el servicio.

B. Garantía

Es importante que la empresa proveedora del dispositivo, ofrezca una garantía durante un período de tiempo razonable, y además ofrezca servicio de garantía en lo posible localmente.

C. Servicio y soporte

Es importante que el proveedor ofrezca servicio y soporte de los equipos que suministra, con una buena respuesta de tiempo para lo cual es importante tenga un centro de servicio y soporte en una localidad cercana.

3.4.4.7 Evaluación de la capacidad de administración del conmutador

Evaluar un conmutador en relación con la administración de la red, envuelve ambas características: la administrabilidad misma del conmutador, y la evaluación de una solución de administración de la red usada para administrar ese conmutador.

Como los conmutadores pueden ser implementados a través de una red, la habilidad para administrar esa red comienza a ser más importante. Será entonces parte importantísima, se cuente con herramientas de sofware y *hardware*, que permitan una administración completa no sólo de estos dispositivos, sino de la red en general, permitiendo que sean analizados patrones de tráfico, monitoreo estándar SNMP, y la capacidad de planificación y afinamiento. Es importante además que se permitan configurar umbrales, los cuales activen alarmas en función de determinada información.

En la sección correspondiente a "Administración del subsistema de conectividad de una red estructurada de datos", en este mismo capítulo, se observarán con más detenimiento algunos detalles, sin embargo a continuación se presentan algunas ideas generales.

Características de administración

El criterio para evaluar las características de administración de un conmutador incluyen:

- Característica de administración en banda[38]
- Característica de administración fuera de banda[39]
- Monitoreo de tráfico
- Soporte MIB

[38] La administración en banda se refiere a aquella administración remota, que puede realizarse a un dispositivo a través de la red desde una estación de trabajo. Normalmente se utiliza la aplicación telnet para administración en banda.

[39] La administración fuera de banda es aquella que requiere que un terminal esté conectado directamente a un puerto serial del dispositivo para su administración, utilizando un interfaz RS-232 generalmente.

a. Característica de administración en banda

Es importante que un conmutador pueda ser administrado en banda, vía TELNET o SNMP (ya sea sobre IP o IPX).

b. Característica de administración fuera de banda

El conmutador debe proveer sesión de consola para administración vía cable RS-232C o por medio de módem usando un emulador de terminal.

c. Monitoreo de tráfico

En una red conmutada, es importante la capacidad de identificar los equipos que más utilizan la red en su momento de carga tope, para localización y optimización. Debería observarse la utilización de la red por tramas, *broadcast*, *multicast* o errores sobre una base por segmento.

d. Soporte MIB

Esta parte será vista con detenimiento en la siguiente sección de este mismo capítulo, sin embargo es importante recalcar que debe ser soportado lo siguiente:

- MIB-II (RFC 1213)
- Interfaces evolution MIB (RFC 1573)
- *Bridge* MIB (RFC 1493)
- RMON MIB (RFC 1557) incluyendo cuatro grupos: estadísticos, históricos, de evento y alarma.

3.4.5 EVALUANDO UN RUTEADOR

Antes de proceder a considerar los aspectos más importante en la evaluación de ruteadores, debe recordarse que estos dispositivos en la actualidad han sido desplazados por los conmutadores como dispositivos de conectividad entre LANs cercanas, debido principalmente a que ofrecen mayor rendimiento (tiempo de latencia), funcionabilidad y costo competitivo. La utilización de ruteadores ha sido desplazada principalmente a lo que es conectividad WAN, sin que esto signifique que estos dispositivos no están en la capacidad de hacer conexiones LANs cercanas, es decir como punto de convergencia de un gran *backbone*. Con frecuencia, los conmutadores presentan opciones que permiten integrar un módulo ruteador dentro del mismo dispositivo, pues si bien el ruteador no provee una alta salida ni baja latencia, son muy útiles cuando se trata de proveer: aislamiento en LANs separadas, decisiones de enrutamiento inteligentes utilizando algoritmos de estado de enlace o vector de distancia, proveer mejor enlace y redundancia, filtración de tráfico sobre protocolos de red y conectividad WAN.

Normalmente, en grandes redes, tanto ruteadores como conmutadores son utilizados juntos para proveer soluciones completas.

Para determinar los requerimientos que debe cumplir un ruteador, deben evaluarse los siguientes criterios:

a. La clase de ruteador que conviene a un medio determinado
b. La arquitectura del ruteador que aseguraría cumplir determinados requerimientos
c. El rendimiento que será capaz de proveer
d. La flexibilidad
e. La confiabilidad
f. La facilidad de administración

3.4.5.1 Clases de ruteadores

Los ruteadores se han clasificado generalmente en las siguientes clases:

1. Ruteador para conexión LAN (punto de convergencia de un *backbone*)
2. Ruteador para conexión WAN

Normalmente, los fabricantes de ruteadores proveen ruteadores que pueden ser configurados modularmente, y el tipo de ruteador que se configure depende más del tipo de conexión para el cual quiere ser utilizado y no de su disponibilidad. Es tan abierto el tipo de configuración que puede obtenerse en un mismo ruteador, que en un mismo dispositivo podrían ser configurados los dos tipos de conexión: para LAN y para WAN.

A. Ruteador para conexión LAN

Estos ruteadores tratan de conectar redes LAN que normalmente se encuentran repartidas en un mismo edificio. Estos ruteadores tienen tablas de direcciones más grandes, y son más flexibles en sus configuraciones de puertos, soportando además salidas con velocidades más altas. Deben soportar topologías LAN tales como: *Token-Ring*, *Ethernet*, FDDI. El ruteador de *backbone* debe ser ampliamente modular y proveer conexiones de alta velocidad (ATM, FDDI, por ejemplo).

B. Ruteador para conexión WAN[40]

Estos ruteadores son diseñados para interconectar un sitio muy grande, y proveer conectividad a servicios remotos. Los ruteadores que soportan este tipo de conexión, son los que en la actualidad tienen mayor acogida, debido a que su función es satisfecha con estos dispositivos que no requieren de respuestas tan rápidas como las de los conmutadores, debido

[40] Recordemos que el tema de estudio de esta tesis son las redes LAN.

a que sus conexiones con enlaces WAN no tienen velocidades de transmisión tan altas como en las redes locales. Los ruteadores que se utilizan para este tipo de conexión deben soportar protocolos de enlace WAN tales como: X.25, *Frame Relay*, SMDS, ATM, SONET, ISDN.

3.4.5.2 Arquitectura de ruteadores

Teniendo establecido lo que un ruteador debe hacer, se puede considerar cual es la arquitectura más apropiada para este dispositivo. La meta principal es proveer piezas independientes de *hardware* para que cada una realice funciones en su turno. Para asegurar el *hardware* para un puerto, debe asegurarse la operación del ruteador tan simultánea como sea posible, lo que permite maximizar el rendimiento del ruteador. Este requerimiento se adapta bien con tecnologías como VLSI, la cual hace fácil replicar bloques de *hardware* (ver figura 3.53). De esta manera, una arquitectura simple tendrá un número de bloques, uno por cada enlace, cada uno de los cuales implementa ambos, un puerto de entrada y uno de salida (del enlace bidireccional). Llamaremos a esto "módulo de enlace". Sobre la entrada el módulo podrá aceptar una cabecera de paquete, realizar el algoritmo de enrutamiento, y requerir una conexión a otro módulo de enlace. Sobre la salida del módulo, se aceptarán cada uno de los paquetes pasados a él a través de una conexión, y opcionalmente borrará uno o dos bytes que pasen a través del filtro del paquete.

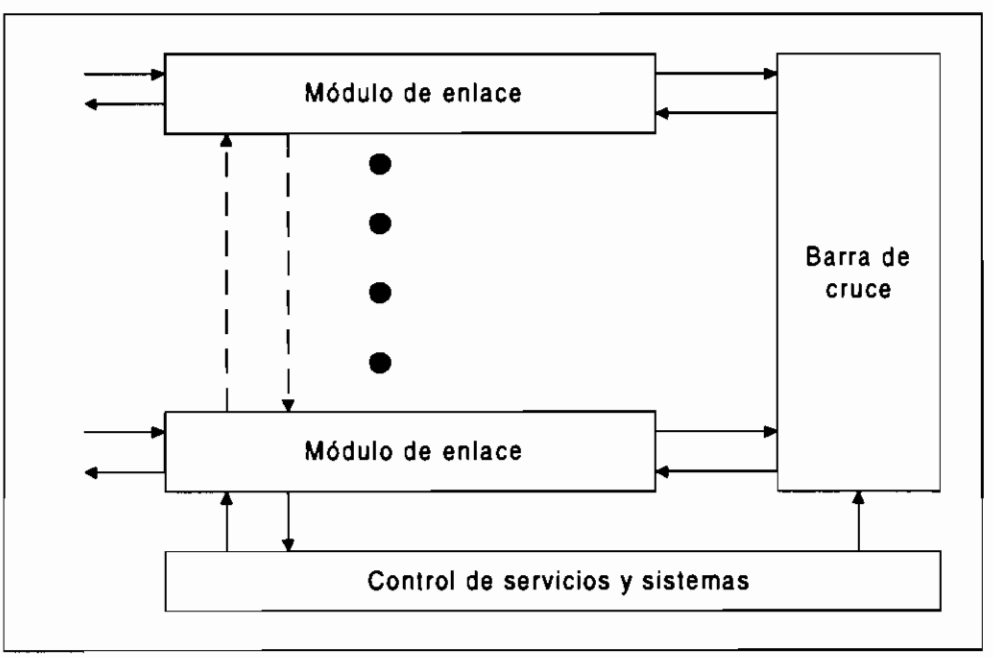


***Figura 3.53** Esquema de conexión de pórticos al bus de un ruteador*

Debería notarse que la provisión de la función de enrutamiento en *hardware* para cada enlace es solamente posible debido a que la implementación de *hardware* del intervalo de enrutamiento es muy pequeña. Esta arquitectura

simple, permite que las funciones de enrutamiento no sean un "cuello de botella" para el rendimiento, y aseguran que el ruteador pueda estar particionado en algunos dispositivos lógicos.

La conexión de los puertos de entrada puede ser hecha por una simple estructura de barra de cruce, la cual no es difícil de implementar en VLSI.

3.4.5.3 Rendimiento de ruteadores

El rendimiento de un ruteador debe medirse principalmente por su capacidad para proveer control de congestión.

El control de congestión, a su vez depende de la segmentación implementada, de las alternativas de enrutamiento disponibles y obviamente de los protocolos de enrutamiento y selección que soporte; pues fundamentalmente serán estos últimos en conjunto con las métricas adoptadas, quienes manejen los recursos primeramente mencionados para obtener un control de congestión óptimo. El ruteador como dispositivo físico, será medido por la cantidad de memoria que soporte y contenga, pues será el parámetro físico que determinará fundamentalmente el grado de tolerancia a grandes congestiones.

3.4.5.4 Evaluando la flexibilidad de un ruteador

Un ruteador de alto rendimiento debe proveer conexiones de altas velocidades para *backbones* y de velocidades lo más altas en lo posible para conectividad WAN. Debido a que un ruteador funcionalmente está relacionado con la capa 3 del modelo de referencia OSI, es importante que soporte el mayor número de protocolos de comunicación de la capa de red, y soporte el mayor número de interfaces de conexión física, especialmente con enlaces WAN.

3.4.5.5 Evaluando la confiabilidad de un ruteador

Cuando se considera confiabilidad, es importante considerar el tiempo de funcionamiento máximo seguro, garantía, servicio y soporte. Los criterios con los que se analiza la confiabilidad de un ruteador, son los mismos que los utilizados en la evaluación de la confiabilidad de conmutadores, explicados en la sección anterior de este capítulo.

3.4.5.6 Evaluación de la capacidad de administración del ruteador

Se utilizarán los mismos criterios que los considerados para la administración de conmutadores, analizados en la sección anterior de este capítulo.

3.5 ADMINISTRACIÓN DEL SUBSISTEMA DE CONECTIVIDAD DE UNA RED ESTRUCTURADA DE DATOS

3.5.1 INTRODUCCIÓN

En la actualidad, las redes soportan nuevas arquitecturas distribuidas, aplicaciones de alto rendimiento, y grandes poblaciones de usuarios, que tienen un impacto significativo sobre la efectividad de las soluciones de administración y requieren de estándares de red que mantengan las ventajas de la tecnología de conectividad.

El subsistema de conectividad debe ser administrado al menos bajo dos puntos de vista: administración de la parte "física" (*hardware*) y administración de la parte "lógica" (*software* y protocolos).

Físicamente, el subsistema de conectividad es mejor administrado actualmente manteniendo políticas de centralización de equipos, las cuales permiten tener los dispositivos de conectividad en grupos organizados que permitan su fácil identificación y cambio si se requiere. Muchas de estas políticas están consideradas en la administración de la infraestructura de transporte, y el subsistema de conectividad, se guía con las mismas políticas. Es importante entonces, que se mantenga una idea concordante y recíproca entre la administración de la infraestructura de transporte y la parte física del subsistema de conectividad.

La administración de la parte lógica, se refiere precisamente a la búsqueda y asignación de estándares que permitan normalizar a todos los proveedores de dispositivos del subsistema de conectividad en determinados protocolos, que permitan la administración de sus dispositivos de una manera abierta. Es decir, un mismo protocolo de administración del subsistema de conectividad, debería ser capaz de administrar cualquier dispositivo perteneciente a dicho subsistema, independiente del fabricante.

En esta sección del capítulo, fundamentalmente nos centraremos en la parte de administración de la parte que hemos llamado "lógica" del subsistema de conectividad, estudiando el funcionamiento de los protocolos de administración de redes más comunes. Debe notarse que la administración del subsistema de conectividad contempla tanto el monitoreo como el control (incluso sobre determinada parte física) de todos sus elementos. El control sobre determinada parte física deberá entenderse como la capacidad de control sobre pórticos, más no sobre ubicación física de los elementos, pues como se explicó anteriormente, las políticas que regirán la administración de la parte "física", serán fundamentalmente las políticas definidas por el sistema de cableado estructurado, y su concepción actual de concentración jerarquizada y organizada de recursos.

La estructura de este numeral ha sido obtenida principalmente de la tesis para doctorado titulada "Network Management Architectures" que está disponible en Internet.

3.5.1.1 Qué es la administración

Existen muchas definiciones de lo que es la administración de la red. La mayoría de estas definiciones son producidas por organizaciones de estandarización, las cuales utilizan su terminología específica de acuerdo a sus campos de aplicación.

Si nos centramos en lo que es la administración del subsistema de conectividad de una red estructurada de datos, la definición que más calza será la siguiente:

"La administración de la red es el acto de inicializar, monitorear y modificar la operación de las funciones de red primarias"

Las funciones de red primarias son aquellas que soportan directamente los requerimientos de usuarios. Ellas permiten por ejemplo a los usuarios accesar a la red, así como encargarse del intercambio de datos del usuario. Durante la fase de diseño, las funciones primarias serán implementadas y realizadas por el diseñador.

La administración, debería inicializar los varios sistemas de red (administración de configuración). Si no ocurren errores, la red inicia el servicio y la fase operacional arranca. Durante esta fase, la administración monitorea los varios sistemas de red para verificar si no ocurren errores. En caso de fallas y mal funcionamiento, los sistemas serán identificados, aislados y reparados (administración de fallas). Si los sistemas no pueden ser reparados, ellos serán reemplazados por nuevos sistemas, los cuales también deberán ser inicializados. Los nuevos sistemas serán añadidos para permitir la conexión de nuevos usuarios, para incrementar el rendimiento o para añadir nueva funcionabilidad. La adición de nuevos sistemas normalmente implica reconfiguración. El monitoreo de la red es también útil para detectar cambios en el flujo de tráfico. Una vez que tales cambios han sido detectados, los parámetros de red podrían ser modificados para optimizar el rendimiento de la red (administración del rendimiento).

Para permitir que las acciones de administración puedan realizarse durante la fase de operación, el diseñador debería definir un número de funciones de administración. Estas funciones deberían ser añadidas en el diseño e implementación para ser realizadas junto con las funciones primarias. Tanto el diseño de las funciones de red primarias como las funciones de administración, pueden ser incorporadas dentro de la misma.

3.5.1.2 Requerimientos de un sistema de administración de una red estructurada de datos

La necesidad de la administración de la red nace fundamentalmente de los requerimientos de los usuarios y puede presentarse como un grupo de funciones a realizar. De aquí, que la selección de un buen sistema de administración de red es importante porque debe satisfacer los requerimientos de los usuarios. Entre las

cosas que deben buscarse en un sistema de administración de red estarán las siguientes:

A. Reducción de costos

Para obtener un buen sistema de administración de red, debe buscarse o diseñarse un sistema que haya sido concebido como multipropósito, es decir que no esté orientado a requerimientos específicos de un único grupo de usuarios, sino por el contrario, lo más general posible para acomodar los requerimientos de muchos potenciales usuarios.

B. Flexibilidad y modularidad

Debido a la velocidad con la que se desarrolla la tecnología, es casi imposible encontrar o implementar un sistema en la fase de diseño, que contemple todo lo que se presentará en la fase de operación. Por esta razón, es una buena idea posponer la búsqueda de soluciones hasta que la fase operacional haya comenzado; resolver tales problemas, será entonces responsabilidad de la administración y del diseño flexible y modular con que haya sido concebido.

En la fase de diseño, los diseñadores se basan en los requerimientos de usuario para obtener sus resultados. De esta manera, la salida del proceso de diseño (en este caso el sistema de administración de red) es primeramente determinado por los requerimientos de usuario.

Sin embargo, hay que recordar que los requerimientos de usuario tienen una naturaleza dinámica, y por tanto el sistema de administración de red deberá permitir también tal dinamismo en la fase de operación.

C. Manejo de fallas

Durante la fase de operación de la red, las fallas pueden ocurrir súbitamente. Las fallas son situaciones en las cuales los componentes de red (o sistemas) no se comportan de la forma en que fueron especificados. Como un resultado de las fallas las redes no pueden proveer sus servicios. La ocurrencia de fallas puede deberse a envejecimiento y decadencia de los componentes de red (*hardware*), así como a errores humanos. Las probabilidades de que las fallas ocurran, dependen de la calidad de los componentes de red y de la forma de trabajo. Por lo general los componentes de mejor calidad son los más caros, sin embargo, ningún fabricante puede proveer hasta el momento componentes que sean buenos por siempre. La forma de trabajo es importante ya que en muchos casos los errores humanos son el resultado de una falta de familiaridad con las circunstancias locales o con determinadas normas.

Debido a que no es posible prevenir todas las fallas y debido a que ellas originan varias consecuencias, la operación de la red debería ser controlada durante la fase operacional por la administración. Tal control envuelve la predicción de fallas potenciales, la detección de fallas existentes, la reducción de los efectos de esas fallas y por supuesto su reparación.

Para la predicción y detección de fallas, los administradores deberían ser capaces de:

- monitorear el comportamiento actual
- comparar el comportamiento actual con el comportamiento previo y/o esperado
- señalar el comportamiento excepcional

Para reducir los efectos de las fallas y permitir su reparación, la administración debe tener los medios para cambiar el estado de la red. Esto debería ser cumplido por el cambio de parámetros de la red.

3.5.1.3 Clasificación de la administración de la red (subsistema de conectividad)

A. Administración explícita e implícita

Un sistema de administración de red puede ser clasificado por la responsabilidad de realización de determinado proceso en el sistema. De acuerdo a este criterio la administración de la red podría clasificarse en:

a. Administración explícita.- Donde los seres humanos son los responsables de la iniciación de las operaciones de administración. De esta forma, serán los operadores quienes se encarguen de iniciar determinadas funciones de administración durante la fase operacional.
b. Administración implícita.- Donde todas las funciones de administración serán realizadas por módulos de *hardware* y *software*. La intervención del operador no será necesaria.

La ventaja de la administración explícita es que no requiere elaborar todas las funciones de administración durante la fase de diseño, debido a que los operadores pueden adaptarse con relativa facilidad a los nuevos requerimientos que se presenten. Por esta razón, estas funciones podrían ser consideradas como la "inteligencia" o "proceso de decisión" de la administración de la red.

Sin embargo, el tiempo de respuesta de la administración explícita será pobre en comparación de la administración implícita.

Si se compara costo y complejidad de las funciones de administración que son elaboradas durante la fase de diseño, las funciones de la administración explícita serán menos caras y complejas que las de la administración implícita. Sin embargo, debido a que la administración explícita requiere de la intervención humana durante la fase de operación, ésta será más costosa que la administración implícita durante la fase de operación.

Como se mencionó en el capítulo anterior, en el numeral 2.5 "Administración de la infraestructura de transporte de una red estructurada de datos", uno de los objetivos del ser humano es dominar totalmente la tecnología tal que ella esté a su servicio pero independiente de él, por tanto se verá que los sistemas de

administración de red deberán tender hacia tipos de administración totalmente implícitos.

B. Administración centralizada y distribuida

La administración centralizada es utilizada para aquellos sistemas en los cuales las decisiones de administración son tomadas por un número limitado de localizaciones centralizadas. Estas decisiones son tomadas por un ente llamado administrador, el cual es considerado como la parte "inteligente" de la administración y en algunas ocasiones se lo refiere como "aplicación" de la administración.

Los agentes son los entes que se encargan de administrar la operación de las funciones primarias. Los agentes representan la funcionabilidad de soporte de la administración a través de los cuales el administrador inicializa, monitorea y modifica el comportamiento de las funciones primarias.

Con la administración centralizada un gran número de sistemas administrados pueden ser controlados por un único sistema administrador.

En la administración distribuida no hay sistemas centrales que se encarguen de tomar las decisiones de administración. Por el contrario, las funciones que toman tales decisiones serán añadidas a los sistemas que ya realizan las funciones primarias.

La característica de la administración distribuida es que cada sistema toma sus propias decisiones de administración. Debido al gran número de sistemas, es virtualmente imposible dejar que los seres humanos tomen esas decisiones; por esta razón, la administración distribuida debe ser realizada de forma implícita.

Una desventaja de la administración distribuida es que será dificultoso cambiarla después de que la fase operacional ha comenzado.

Al contrario de la administración distribuida, la administración centralizada puede realizarse de forma implícita o explícita. Una desventaja de la administración centralizada es que la red entera podría quedar fuera de control luego de una falla en el único administrador. Adicionalmente la administración centralizada es menos eficiente que la administración distribuida ya que el administrador central debe intercambiar información con todos los agentes.

3.5.1.4 Arquitectura de un sistema de administración de redes

Un sistema de administración de redes contiene: algunos (potencialmente muchos) nodos, cada uno con una entidad de procesamiento, denominado agente, el cual tiene acceso a instrumentación de administración; al menos una estación de administración-administrador *(NMS-Network Management Station);* y un protocolo de administración, usado para convertir información de administración entre los agentes y las estaciones de administración. Las operaciones del protocolo

son guiadas bajo una armazón administrativa la cual define tanto políticas de autenticación como de autorización.

Las estaciones de administración ejecutan las aplicaciones de administración las cuales monitorean y controlan elementos de la red. Los elementos de la red son dispositivos tales como *hosts*, ruteadores, servidores de terminal, etc, los cuales son monitoreados y controlados a través del acceso a su información de administración.

La información de administración es vista como una colección de objetos administrados, residentes en una almacenadora virtual de información, denominada Base de la información de administración *(MIB-Management Information Base)*. Las colecciones de los objetos relatados están definidos en *módulos MIB*. Estos módulos son escritos utilizando un subgrupo de notaciones de sintaxis definidas por la *ASN.1 (Abstract Syntax Notation One)* de OSI, en la denominada Estructura de Información de Administración *(SMI-Structure of Management Information)*.

Cuando se diseña un módulo MIB, es útil que las nuevas definiciones se hagan similares a las definidas en el SMI. En comparación al tipo definido en el SMI, cada uno de estos nuevos tipos tiene un nombre diferente, una sintaxis similar, pero semántica más precisa. Estos nuevos tipos son definidos como convenciones textuales, y son usadas para conveniencia de los humanos y su capacidad de leer módulos MIB.

El modelo de arquitectura de administración se muestra en la figura 3.54.

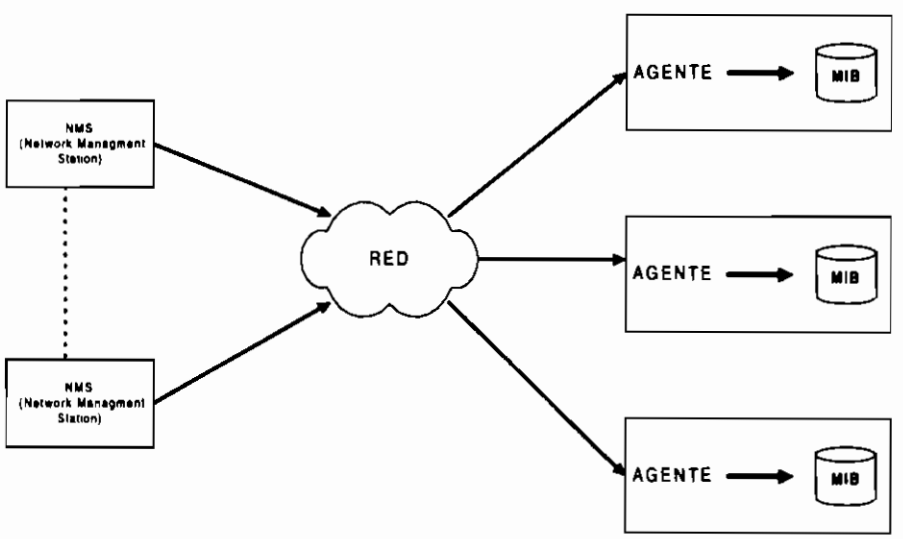


***Figura 3.54** Modelo de la arquitectura de administración de la red*

El agente, típicamente realiza lo siguiente:

- Implementa completamente el protocolo

- Almacena y recupera datos de administración como hayan sido definidos por el MIB
- Puede asincrónicamente indicar un evento al administrador
- Puede ser un paso intermedio para algunos nodos de red no SNMP administrables

El administrador usualmente:

- Es implementado como un NMS (*Network Management Station*)
- Implementa completamente el protocolo
- Es capaz de hacer requerimientos a agentes
- Configura variables en agentes
- Realiza reconocimiento asincrónico de eventos que vienen desde los agentes

Algunos fabricantes reconocidos mundialmente, ofrecen plataformas de administración de red, las cuales implementan el rol del administrador (listados en orden alfabético):

- *Dec Polycenter Network Manager*
- *Hewlett Packard Open View*
- *IBM AIX NetView/6000*
- *SunConnect SunNet Manager*

3.5.2 ESTÁNDARES DE SISTEMAS DE ADMINISTRACIÓN DE REDES

Como se conoce, existen algunas organizaciones tales como ISO, ITU-T (anteriormente CCITT), IETF que se encargan de desarrollar servicios, protocolos y arquitecturas para la administración de la red.

Debido a la importancia que se le ha dado al modelo de referencia OSI en esta tesis, se considerará el estándar de administración de redes de OSI de ISO para ser tratado a continuación. Adicionalmente, se hará referencia al estándar de administración TMN introducido por ITU para ser brevemente comparado con el anterior.

Finalmente se estudiará el estándar de administración de Internet (relacionado con SNMP), debido a la importancia que tiene por su difusión a escala mundial.

3.5.2.1 Administración OSI

El origen de la administración OSI puede ser encontrado en ISO, la mayoría del trabajo es realizada en colaboración con ITU-T. En 1980 un grupo especial de trabajo fue formado dentro de ISO para desarrollar la administración de OSI. El primer resultado que tuvieron se lo conoce como OSI *Management Framework.*

Debido al gran tiempo que tomó este estándar no fue ampliamente aceptado, y se decidió producir un estándar adicional llamado *Systems Management Overview*.

A. OSI Management Framework

En este estándar se consideran 3 aspectos principales:

- Areas funcionales
- Intercambio de la información de la administración
- Objetos administrados, información de administración y el MIB

A.1 Areas funcionales

Las funciones de administración son conocidas como las 5 áreas funcionales de OSI:

Fault Management (Administración de fallas)
Configuration Management (Administración de configuración)
Accounting Management (Administración de contabilidad)
Performance Management (Administración de rendimiento)
Security Management (Administración de seguridad)

Por esta razón son conocidas las siglas en inglés FCAPS.

A.1.a Administración de fallas

Es el grupo de facilidades que habilitan la detección, aislamiento y corrección de operaciones anormales de la red. Las funciones que incluye son:

- Mantener y examinar registros de errores
- Aceptar y actuar bajo notificaciones de error
- Detectar e identificar fallas
- Obtener pruebas de diagnóstico
- Corregir fallas

A.1.b Administración de configuración

La administración de la configuración es el grupo de facilidades las cuales:

- Registran la configuración actual
- Registran los cambios en la configuración
- Identifican los componentes de red (dan direcciones a Puntos de Acceso a Servicios -SAP- y nombra a entidades de red)
- Inicializa y apaga los sistemas de red
- Cambia los parámetros de red (ej: tablas de ruteo)

Un aspecto importante de la administración de la configuración es la asignación de nombres.

A.1.c Administración de contabilidad

Es el grupo de facilidades que habilitan las cargas a ser establecidas, y costos a ser identificados para el uso de los recursos de red. Estos recursos son:

- Proveedor de servicio de red, el cual es responsable de la transferencia de datos de usuario
- Servicios de red (servicio de impresión, servicio de directorios, servicio de correo electrónico, etc)

La administración de la contabilidad debería:

- Informar a los usuarios de los costos que utilizan
- Informar a los usuarios de los costos esperados en el futuro
- Configurar límites de costos (ej. limitar extensiones telefónicas)
- Combinar costos para prevenir que los usuarios reciban cuentas separadas por cada conexión individual.

A.1.d Administración del rendimiento

La administración del rendimiento es útil para optimizar la calidad de servicio (QoS). Para detectar cambios en el rendimiento, es necesario contar con registros de datos estadísticos que hayan sido tomados periódicamente durante determinado tiempo. Además estos registros pueden ser utilizados para detección de fallas (administración de fallas), para decidir cuando son necesarios cambios en la configuración (administración de configuración) y para ajustes de cuentas (administración de contabilidad).

A.1.e Administración de seguridad

Es el grupo de facilidades que habilitan al administrador iniciar y modificar las funciones de seguridad de la red por mal funcionamiento de usuarios y accesos no autorizados. Las partes importantes de la administración de seguridad son la administración de claves, mantenimiento de *firewalls*, y creación de registros de seguridad.

A.2 Intercambio de la información de administración

El modelo de referencia OSI presenta tres formas diferentes de realizar el intercambio de información:

- Administración de sistemas
- Administración de capas
- Administración de aplicaciones

A.2.a Administración de sistemas

Hace distinción entre dos diferentes propiedades:

- La administración de sistemas es relativa a la administración de los recursos OSI y a su estado a través de todas las capas de la arquitectura OSI
- Los protocolos para la administración de sistemas reside en la capa de aplicación

La administración de sistemas puede ser caracterizada por el factor de que esos protocolos de aplicación deberían ser utilizados para el intercambio de la información de administración, y además, según su visión, el intercambio de la información de administración debería realizarse como cualquier otro tipo de información.

Para modelar el cambio de la información de la administración, se introdujo el concepto de *Systems Management Application Entities* (SMAE) el cual reside en la capa de aplicación y realiza los aspectos de comunicación de las funciones de administración de sistemas.

Los argumentos que defienden el intercambio de la información de la administración en el nivel de aplicación son los siguientes:

- Los protocolos de la capa de aplicación son los tipos de protocolos más poderosos. Un solo protocolo en la capa de aplicación será capaz de transferir muchos tipos de información de administración. Definir un solo protocolo poderoso es mucho mejor que definir muchos protocolos de poca importancia.
- Los servicios provistos por las capas más bajas comúnmente no son los suficientemente buenos para satisfacer todas las necesidades de red.
- La administración es vista como una aplicación en el tope de la red.

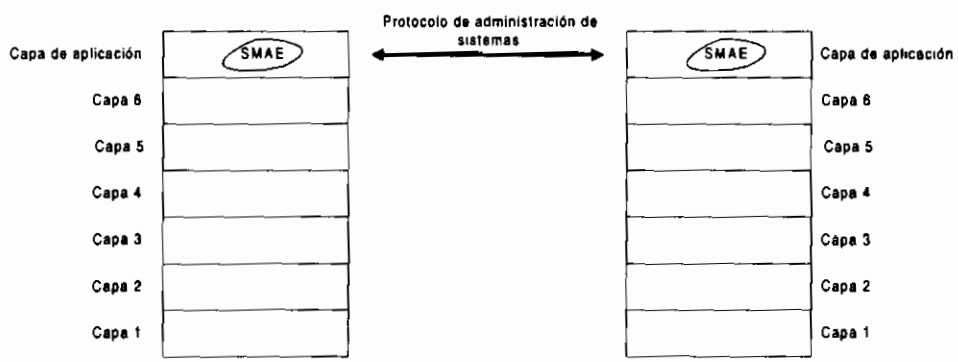


***Figura 3.55** Systems Management Application Entities (SMAE) en la capa de aplicación*

Los argumentos que se oponen al intercambio de información de administración en el nivel de aplicación son:

- La implementación de las siete capas del modelo de referencia es costosa. Hay muchos sistemas que para su operación normal no necesitan implementar las 7

capas (ej: ruteadores, *hubs*, *switches*). Sería un desperdicio de dinero implementar las 7 capas en estos sistemas solo para la administración.

- Si un problema ocurriera con la red y los protocolos de la capa de aplicación no pudieran funcionar bien los servicios de la red no podrían ser restaurados hasta que estos protocolos funcionen bien.
- Los protocolos de la capa de aplicación envuelven muchos procesos y son relativamente lentos
- Los protocolos de la capa de aplicación no tienen facilidades de *broadcast* y *multicast*

A.2.b Administración de capas

El OSI *Management Framework* permite como alternativa la administración de capas, que tiene las siguientes propiedades:

- La administración de la capa n soporta el monitoreo, control y coordinación de los objetos administrados de la capa n.
- Los protocolos de la capa n son soportados por protocolos de las capas n-1 e inferiores.

La primera propiedad nos dice qué está siendo administrado, mientras que la segunda nos dice *cómo* la información de la capa n podría ser intercambiada.

Una diferencia importante entre la administración de sistemas y administración por capas, es que la primera utiliza el servicio de presentación para el intercambio de la información de la administración, mientras que la administración de la capa n utiliza el servicio de la capa n-1. De acuerdo al *OSI Management Framework*, el uso de la administración por capas se realizará cuando no sea apropiado implementar la administración de sistemas (ej: en ruteadores, ya que requieren funciones de *broadcast*).

A.2.c Operación de capas

La operación de capas es definida como el monitoreo y control de una única instancia de comunicación[41]. En la operación por capas, la información de administración es llevada como parte de un protocolo de capa normal. Solo como con la administración de la capa n, la operación de la capa n usa los protocolos de las capas inferiores para el cambio de la información de administración.

A.3 Objetos administrados, información de administración y el MIB

A lo largo de la evolución del *Management Framework* se ha ido dando definiciones de objetos administrados e información de administración.

[41] Una única instancia de comunicación es una única conexión (en el caso de servicio orientado a conexión) o un único par requerimiento-respuesta (en el caso de un servicio sin conexión)

- Objetos administrados son los recursos de procesamiento y comunicación de datos (pueden o no ser recursos OSI) que deberían ser administrados a través del uso de un protocolo de administración OSI.
- Información de la administración es la información asociada con un objeto administrado que es operado por el protocolo de administración para controlar y monitorear ese objeto.

Además se han dado algunas opiniones emergentes que dicen:

- Los objetos administrados residen en varias capas del modelo de referencia OSI
- La información de administración reside en el MIB

El MIB puede ser visto como un tipo de base de datos que contiene la información *asociada* con los objetos administrados. Las capas de administración son las responsables de mantener la asociación entre la información del MIB y los objetos administrados.

B. OSI Systems Management Overview

El SMO (*Systems Management Overview*) fue introducido en 1991 (empezó en 1987), y comparado con el OSI *Management Framework,* SMO tiene mayor aceptación porque tiene mayor información.

El SMO incluye mayor descripción de la administración de sistemas. Esta descripción distingue entre los siguientes aspectos:

- De información
- Organizacionales
- Funcionales
- De comunicación

B.1 Aspectos de información

Los aspectos de información del modelo de administración de sistemas tienen que ver con los objetos que están siendo administrados. Estos recursos son vistos como 'objetos administrados'.

El concepto de objetos administrados fue introducido como parte del *Management Framework* de OSI. Debido a inexactitudes en el concepto, se dieron varias interpretaciones del mismo, por lo que se decidió redefinirlo:

> "Un objeto administrado es una vista de administración de OSI de un recurso que está sujeto a administración, tal como en la entidad de capas, una conexión o un elemento del equipo físico de comunicaciones. Así, un objeto administrado es la abstracción de tal recurso que representa sus propiedades como son vistas por la administración. Una parte esencial de la definición de un objeto administrado es la relación entre estas propiedades y el

comportamiento operacional del recurso. Esta relación no es modelada de una manera general"

De acuerdo al Modelo de Información de Administración de OSI la vista de administración de un objeto administrado está descrita en términos de:

- Atributos, los cuales son propiedades o características del objeto
- Operaciones, las que se realizan sobre el objeto
- Comportamiento, el cual es exhibido en respuesta a las operaciones
- Notificaciones, las cuales son emitidas por el objeto

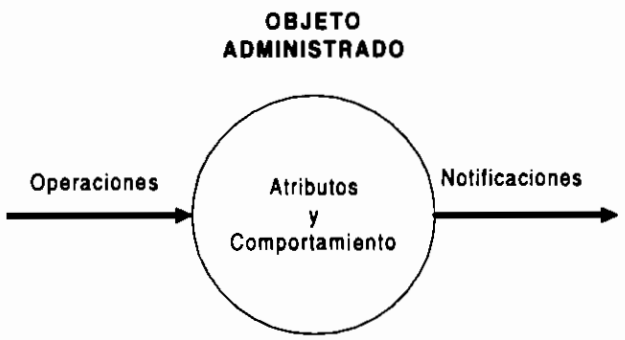


Figura 3.56 Diagrama de entradas y salidas de un objeto administrado

B.2 Aspectos organizacionales

La administración de sistemas OSI está organizada de una manera centralizada. De acuerdo a este esquema, un único administrador puede controlar algunos agentes. La figura 3.57 ilustra el concepto administrador-agente.

El ambiente de administración OSI puede ser dividido en un número de dominios de administración. La división puede realizarse basada en requerimientos funcionales (por ejemplo: seguridad, manejo de fallas) o de otros requerimientos (geográficos o tecnológicos).

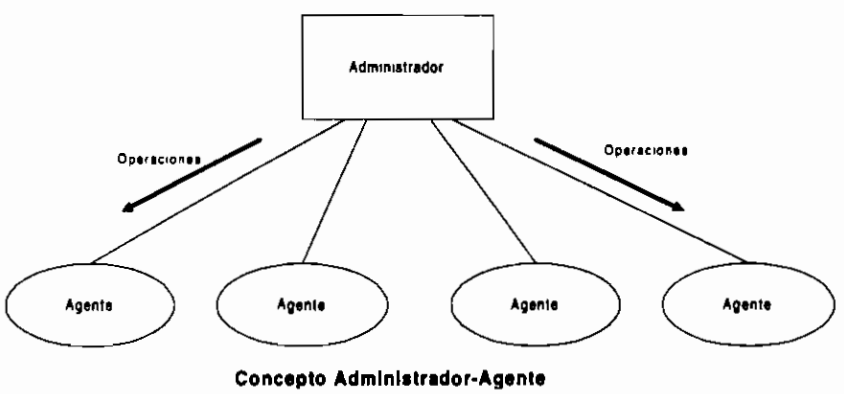


Figura 3.57 Relación jerárquica administrador-agente

B.3 Aspectos funcionales

Tan pronto como el primer trabajo del *Management Framework* apareció, ISO comenzó a definir protocolos estándares para cada una de las cinco áreas funcionales (FCAPS). La mayoría de protocolos de área funcional usaron un grupo similar de funciones de administración elementales. Por esta razón se decidió detener el desarrollo de protocolos para esas cinco áreas funcionales y se concentró sobre la definición de las funciones de administración elementales.

Las funciones de administración elementales, las cuales son definidas en un nivel de abstracción más bajo que las áreas funcionales originales, son llamadas 'Funciones de Administración de Sistemas' (cuyas siglas en inglés son SMF). Estas funciones son varias, entre las que se puede listar: función de administración de objeto, función de administración de estado, atributos para relaciones de representación, función de reporte de alarma, y otras. Todas estas funciones se encuentran estandarizadas tanto en ISO/IEC así como en ITU-T.

B.4 Aspectos de comunicación

OSI ha definido el CMIS (*Common Management Information Service*) como el servicio preferido para el cambio de la información de administración. El CMIS está restringido a la transferencia de la información de administración; el control de sistemas se ha dejado a los usuarios del MIS, los cuales están localizados sobre el CMIS.

El estándar CMIS define las siguientes primitivas de servicio: M-GET, M-CANCEL-GET, M-SET, M-ACTION, M-CREATE, M-DELETE, M-EVENT-REPORT.

La interacción entre los SMAEs es definida por el '*Common Mannagement Protocol*' (CMIP).

El protocolo CMIP fue creado para remplazar a SNMP a finales de los 80. Desgraciadamente, problemas con su implementación demoraron su amplia disponibilidad y ahora está solamente disponible en forma limitada desde sus propios desarrolladores.

CMIP fue diseñado para construirse sobre SNMP y formar un administrador de red más detallado. Su diseño básico es similar a SNMP, empleando PDU como variables para monitorear una red. CMIP sin embargo contiene 11 tipos de PDUs (en comparación con los cinco de SNMP).

En CMIP, las variables son vistas como muy complejas y sofisticadas estructuras de datos, con muchos atributos.

Ventajas de CMIP

La principal ventaja de CMIP es que sus variables no solamente son de espera de información, sino que poseen características más activas que SNMP. Por ejemplo,

si una estación no puede alcanzar un determinado servidor por repetidas ocasiones, entonces CMIP notificará al personal apropiado de ese evento.

CMIP tiene construidos dispositivos de gestión de seguridad que soportan autorización, control de acceso y logs de seguridad. El resultado de esto es un sistema más seguro desde la instalación de CMIP; no son requeridas actualizaciones de seguridad como en SNMP.

Otra ventaja es que CMIP fue fundado no solamente por organizaciones gubernamentales, sino también por grandes corporaciones. La una puede inducir a que no tenga un gran desarrollo dentro del mundo de los negocios, pero cuando ya tiene su disponibilidad amplia, tendrá numerosos usuarios inmediatos, tales como las organizaciones y corporaciones que lo fundaron.

Desventajas de CMIP

CMIP toma una mayor cantidad de recursos del sistema que SNMP en un factor de 10 (mientras SNMP requiere tan solo de 70 Kbytes de memoria, CMIP requiere de 700 Kbytes aproximadamente). Muy pocos sistemas son capaces de manejar una implementación completa de CMIP sin una modificación masiva de la red. Esto provoca que su implementación resulte en una inversión muy costosa, lo que se convierte en su mayor desventaja. Para disminuir sus costos, el protocolo debería cambiar sus especificaciones.

Otro problema es que es muy difícil de programar, debido a la gran cantidad de variables que posee.

Discusión sobre la administración OSI

Un problema importante de la arquitectura de administración de OSI es que no se aplican los principios del modelo de referencia de OSI, especialmente el relacionado con la división en capas, el cual dice que los usuarios en una capa en particular no necesitan conocer la estructura interna de sus proveedores de servicio de capas inferiores.

Deben considerarse dos sistemas: un administrador y un agente. El sistema que opera como agente es el que está siendo administrado, y contiene algunos objetos administrados para representar los recursos que pueden ser administrados. Los objetos administrados pueden ser accesados por un SMAE (*Simple Management Application Entitie*). Este SMAE se comunica con otro que está en el sistema administrador a través de un protocolo de administración de sistemas (CMIP).

Cada capa del modelo de referencia OSI puede necesitar administración. Los objetos administrados pueden así ser encontrados en todas las capas del modelo de referencia OSI. El SMAE está ubicado por definición en la capa de administración (capa 7), pero puede manipular objetos administrados independiente de la capa donde se encuentren, por lo que debería conocer la estructura interna del resto de capas, lo que va en contraposición de las leyes del modelo de referencia OSI.

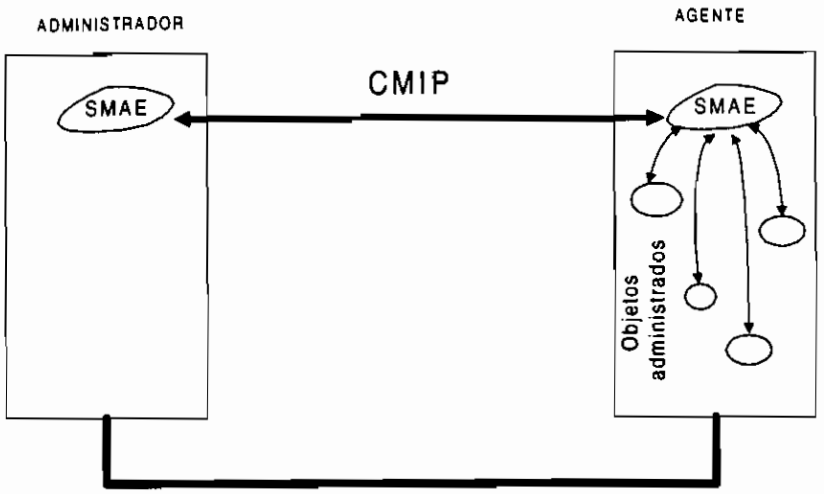


Figura 3.58 Comunicación entre un sistema administrador y un agente utilizando el protocolo CMIP

Adicionalmente, el que el SMAE se encuentre en la capa 7 puede presentarse como otro problema con la administración de fallas. Esto se debe principalmente a que los protocolos que están siendo administrados, son también usados para el intercambio de información de administración. El problema con está dependencia es que en algún momento en que fallen las estructuras de las capas más bajas (3, 4 por ejemplo), el SMAE podrá detectar la falla, sin embargo estará imposibilitado de transmitir una alarma debido a que no tiene un camino para transportarlo hasta que las mencionadas capas (3,4) se recuperen de la falla. De esta manera la administración de fallas sería imposible.

Entre otros problemas, uno de los principales para que este modelo de administración no haya sido fácilmente aceptado, es que tomó demasiado tiempo su estandarización y se realizaron demasiados cambios, y muchos de los conceptos son difíciles de comprender. Además, la administración OSI explica cómo podrían realizarse las operaciones de administración, pero no especifica en qué secuencia.

3.5.2.2 Administración TMN (Telecommunications Management Network)

El término TMN fue introducido por el ITU-T (CCITT) en la recomendación M.3010. TMN conceptualmente es una red separada que actúa como interfaz con una red de telecomunicaciones en algunos puntos diferentes. Los puntos de interfaz entre el TMN y la red de telecomunicaciones están formados por sistemas de intercambio y transmisión. Para el propósito de administración, estos sistemas de intercambio y transmisión están conectados por medio de una red de comunicación de datos a uno o más sistemas de operaciones.

La red de comunicación de datos es usada para intercambiar información de administración entre los sistemas de operación y es también utilizada para conectar estaciones de trabajo.

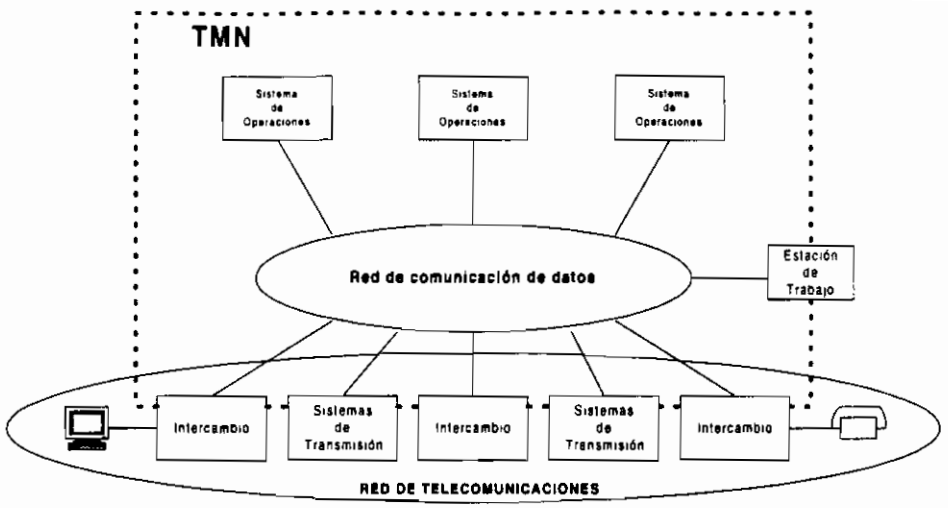


***Figura 3.59** Esquema de administración TMN*

Luego de la publicación de la recomendación M.3010, la colaboración entre el CCITT e ISO/IEC fue mejorada, y se incorporaron nuevas ideas al TMN. Entre los principales cambios estuvieron:

- Se adoptó el concepto 'Administrador-Agente'.
- Se adoptó además el concepto de 'Orientado a objetos' de ISO
- Se incluyó la idea de 'Administración de dominios'.

A pesar de esta cooperación, se mantiene una diferencia fundamental, y es que el grupo de administración ITU prefiere introducir una red separada para transferir la información de administración. Se debe recordar que el grupo ISO utiliza los mismos componentes para la red que es administrada y la red sobre la cual la información de administración es transferida. La ventaja de mantener una red separada para funciones de administración, es que se garantiza de mejor manera la administración de fallas en caso de que éstas ocurrieran en la red normal; sin embargo se presenta una gran desventaja y es que la falla podría presentarse en la red separada de administración, por lo que debería garantizarse que esta red sea muy segura y por lo tanto muy costosa.

Una diferencia interesante entre OSI y TMN es que OSI ha definido una única arquitectura de administración mientras que TMN define múltiples arquitecturas en niveles diferentes de abstracción (arquitectura funcional y arquitectura física).

Otra diferencia es que TMN provee una estructura para los múltiples niveles de responsabilidad de administración que existen en las redes reales (se definen las siguientes capas: capa de elemento de red, capa de administración de elemento de red, capa de administración de red, capa de administración de servicio, capa de administración de negocios); la administración OSI no provee tal estructura. La estructura TMN es conocida como 'modelo de responsabilidad', y su principal ventaja es que hace más fácil el entendimiento y distinción de varias responsabilidades de administración.

3.5.2.3 Administración Internet

En 1987 tres propuestas de administración aparecieron: *High-level Entity Management System / Protocol* (HEMS/HEMP), *Simple Network Management Protocol* (SNMP) y *Common Management Over TCP/IP* (CMOT). En marzo de 1988 se decidió que se utilizará SNMP para el corto plazo y CMOT (de los estándares OSI) para largo plazo. Sin embargo CMOT encaró los mismos problemas que la administración OSI (con su protocolo CMIP) pero en ambiente Internet, siendo éste el hecho para que las especificaciones no aparecieran a tiempo.

El éxito de SNMP se debe fundamentalmente a que el grupo IETF no le dedicó mucho tiempo a los diseños arquitecturales, sino que se dedicó al desarrollo e implementación del protocolo, lo que no ocurría con el grupo de trabajo de ISO. Por esta razón se explica que no existan estándares especiales para la arquitectura de administración de Internet. Sin embargo se ha escrito mucho sobre la administración Internet, y de ahí que pueda resumirse lo siguiente:

- Todos los sistemas deberían ser administrables vía SNMP
- El costo de añadir sistemas de administración de red debe ser mínimo
- Debe ser fácil extender las capacidades de administración de sistemas existentes (extendiendo los MIB)
- La administración de red debe ser robusta. En caso de falla, un pequeño grupo de capacidades de administración debe estar disponible

Aparentemente SNMP fue la solución correcta en su momento. Sin embargo, en 1992 se desarrolló una versión mejorada de SNMP y se la llamó SNMPv2. Los dos protocolos dicen cómo debería ser cambiada la información, pero ninguno dice *cual* información de administración existe. Esa información está definida por los varios estándares de MIB.

A. Protocolo SNMP

SNMP está basado en el modelo administrador/agente. SNMP es referido como "simple" debido a que el agente requiere un *software* mínimo. La mayoría de las fuentes de procesamiento y de almacenamiento de datos residen sobre el sistema de administración, mientras que un subgrupo complementario de esas funciones reside en el sistema administrado.

Para obtener su meta de ser simple, SNMP incluye un grupo limitado de comandos y respuestas de administración. El sistema de administración resuelve mensajes Get, GetNext y Set para restaurar variables de objeto individuales o múltiples o para establecer el valor de una variable individual. El agente administrado envía un mensaje de respuesta para completar los mensajes Get, GetNext o Set. El agente administrado envía una notificación de un evento, llamada *trap* al sistema de administración, para identificar la ocurrencia de condiciones tales como umbrales que han excedido un determinado valor. En resumen hay solamente 5 operaciones primitivas:

1. Get (operación de recuperación)
2. GetNext (operación transversal)
3. Get Response (operación indicativa)
4. Set (operación alterna)
5. *Trap* (operación *trap* asincrónica)

A.1 Construcción del mensaje SNMP

Cada mensaje SNMP tiene el siguiente formato:

- Número de versión
- Nombre de la comunidad (*Community Name*)
- Tipo de *password*
- Uno o más PDUs SNMP - asumiendo autenticación trivial

Cada PDU SNMP excepto el *trap* tiene el siguiente formato:

- Requerimiento de identificación (*Request id*)
- Requerimiento del número de secuencia
- Estado de error (cero si no hay error)
- Indice de error (si no es cero indica cual OIDs en el PDU causó el error)
- Lista de los OIDs y valores (los valores son nulos para el *get* y *getnext*)

Los PDUs *trap* tienen los siguientes mensajes:

- Empresa - identifica el tipo de objeto que causa el *trap*
- Dirección de agente - la dirección IP del agente el cual envía el *trap*
- Identificación del *trap* genérico - los *trap* estándares comunes
- Identificación del *trap* específico - *trap* propietario o de empresa
- Marca de tiempo - cuando el *trap* ocurrió en *ticks* de tiempo
- Lista de OIDs y valores - OIDs que podrían ser reelevantes para enviar al NMS

Fuera de línea del protocolo SNMP

- Cada objeto administrado SNMP pertenece a una comunidad
- La estación NMS podría pertenecer a múltiples comunidades
- Una comunidad está definida por un nombre de comunidad, el cual es una serie de octetos con una longitud entre 0 y 255 octetos.
- Cada mensaje SNMP consiste de tres componentes:
    - Número de versión
    - Nombre de la comunidad
    - Datos - una secuencia de PDUs asociados con el requerimiento

A.2 Niveles de seguridad con el SNMP básico

Autenticación:

- La autenticación trivial basada en el plan del nombre de la comunidad de texto en mensajes SNMP
- La autenticación está basada en la suposición de que el mensaje no está corrupto

Autorización

- Una vez que el nombre de comunidad es validado, el agente o administrador verifica si la dirección de envío está permitida o tiene derechos para la operación requerida
- Una vista o un corte ("View" o "Cut") de los objetos, junto con los derechos de acceso permitidos, son enviados al administrador cuyo nombre de comunidad y dirección de envío se conocen.

A.3 A qué accesa SNMP?

- SNMP accesa a momentos particulares de un objeto
- Todos los momentos de un objeto en el MIB residen en los nodos terminales de árbol MIB
- El protocolo SNMP accesa objetos formando un objeto identificador de la forma *x.y*, donde *x* es el "verdadero" OID para el objeto en el MIB, y *y* es el sufijo especificado por el protocolo que identifica únicamente un momento particular (ej: cuando está accesando a una tabla).
- Para un momento primitivo único los objetos terminales usan *y=0*. Por ejemplo, sysDescr (OID: 1.3.6.1.2.1.1.1) podría ser referido en el protocolo SNMP por 1.3.6.1.2.1.1.0 (es decir sysDescr.0)
- Para un momento único de objetos terminales en columnador (es decir un momento del tipo de tabla de un objeto) usa y=I1.I2.I3... (Ii son los índices de las tablas) por ejemplo: el MIB transversal utilizando la operación GetNext

A.4 Ventajas de SNMP

La ventaja más grande que tiene SNMP es su diseño simple, debido a que es fácil de implementar sobre grandes redes, sin que tome demasiado tiempo configurarlo ni produzca *stress* sobre la red. Además, su diseño simple hace fácil que un usuario pueda programar las variables que podrían ser monitoreadas, para que en un nivel de perspectiva más bajo cada variable consista de la siguiente información:

- el título de la variable
- el tipo de dato de la variable (ej: entero, caracter)
- dónde la variable es sólo lectura o sólo escritura
- el valor de la variable

El resultado de su simplicidad es un administrador de red fácil de implementar y que no carga demasiado la red existente.

Otra ventaja es que es de muy amplia difusión. El resultado de esto es que la mayoría de proveedores de *hardware* de conectividad, tales como puentes, conmutadores y ruteadores, hacen productos que soporten SNMP, haciendo fácil su implementación.

La expandibilidad es otro beneficio de SNMP. Debido a su diseño simple, es fácil para el protocolo ser actualizado y así expandirse a las necesidades de los usuarios en el futuro.

A.5 Desventajas de SNMP

La primera deficiencia de SNMP es que tiene algunas falencias grandes en cuanto a seguridad que pueden dar acceso a intrusos de red a la información llevada a lo largo de la red. Los intrusos podrían dar de baja algunos terminales.

La solución a este problema es simple. Debido a la expandibilidad de SNMP, la última versión de SNMP, llamada SNMPv2, tiene añadidos algunos mecanismos de seguridad que ayudan a combatir los problemas más grandes de seguridad:

- Privacidad de datos (para prevenir que intrusos accesen a la información llevada a través de la red)
- Autenticación (para prevenir que intrusos hagan envíos falsos de datos a través de la red)
- Control de acceso (para restringir acceso de variables particulares a ciertos usuarios, removiendo la posibilidad de que un usuario accidentalmente detenga el servicio de red)

El problema más grande con SNMP es que es considerado tan simple que la información que distribuye nunca está detallada ni organizada lo suficiente para distribuir datos en grandes redes como son las de los 90.

Este nuevo problema ha sido arreglado con la nueva versión SNMPv2, la cual permite más detalle de variables, incluyendo el uso de la tabla de estructura de datos para facilitar la recuperación de datos. También son incluidas dos nuevas PDUs que son usadas para manipular los objetos contenidos en tablas. En efecto, muchas nuevas características han sido añadidas, expandiendo sus especificaciones desde 36 páginas (con la versión inicial) a 416 páginas (para SNMPv2). Algunos podrían decir que SNMPv2 perdió su principal característica: su simplicidad, sin embargo, esos cambios fueron necesarios para las grandes redes de esta década (los 90).

Podría pensarse además, que SNMPv2 es la solución. Sin embargo, SNMPv2 para muchos autores no queda más que en la teoría. SNMPv2, falló principalmente debido a que no enfrenta facetas claves como: no se encuentra fácilmente un administrador ni un agente SNMP que soporten completamente las complejas

extensiones propuestas por v2. Muchos autores piensan que SNMPv2 falló debido a que era muy exigente.

A.6 Protocolos de comunicación fundamentales

SNMP asume que el camino de comunicación es una subred de comunicación no orientada a conexión, es decir, no hay un camino de comunicación preestablecido para la transmisión de datos. Como resultado, SNMP no garantiza la entrega confiable de datos, aún cuando la mayoría de los datos obtendrán salida, y los que no, podrán ser retransmitidos. Los protocolos primarios que SNMP implementa son UDP (*User Datagram Protocol*) e IP (*Internet Protocol*). SNMP también requiere protocolos de la capa de enlace de datos tales como *Ethernet* o *Token-Ring*, para implementar el canal de comunicación desde el administrador al agente administrado.

La simplicidad de SNMP y la comunicación no orientada a conexión también produce un grado de robustez. Ni el administrador ni el agente cuentan el uno con el otro para esta operación. Así, un administrador podría continuar funcionando aunque el agente remoto falle. Cuando el agente vuelve a funcionar, aquel puede enviar un *trap* al administrador, notificándole del cambio en su estado operacional. La naturaleza de no orientarse a conexión de SNMP deja la recuperación y la detección del error al NMS (*Network Management Station*) y al agente. Sin embargo, debe recordarse que SNMP es en la actualidad independiente del transporte y pueden ser implementado sobre otros transportes tales como: TCP, mapeo directo sobre el nivel MAC de *Ethernet*, encapsulamiento en el protocolo X25, encapsulamiento en celdas ATM, y así.

La figura 3.60 describe el mecanismo de transporte usado por SNMP sobre UDP.

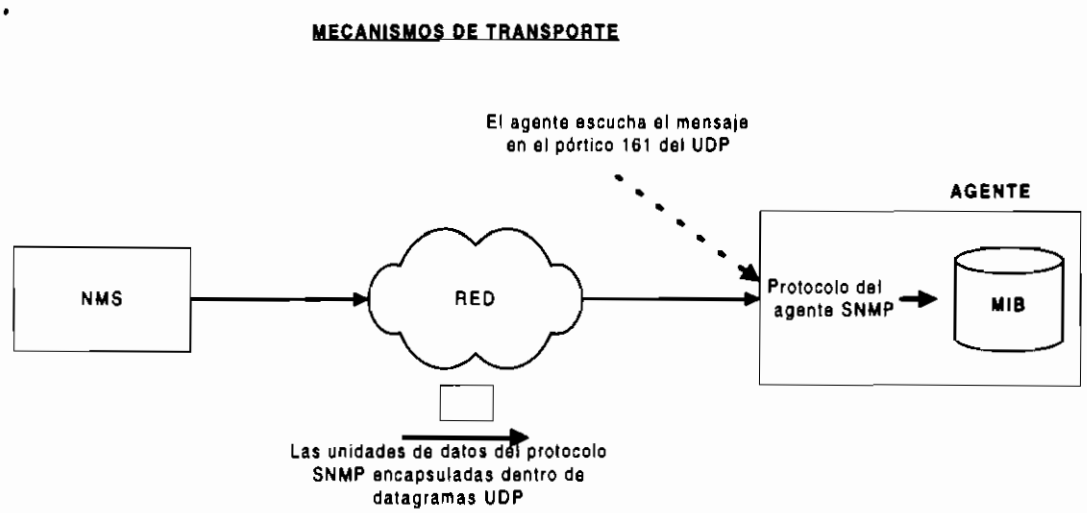


***Figura 3.60** Mecanismo de transporte usado por SNMP sobre UDP*

Transporte UDP

- El agente escucha sobre el pórtico 161 de UDP
- Las respuestas son enviadas de regreso al pórtico del NMS de origen desde un pórtico dinámico, la mayoría de agentes usan el pórtico 161 para este propósito
- El tamaño máximo del mensaje SNMP está limitado por el tamaño máximo del mensaje UDP (es decir 65507 octetos)
- Todas las implementaciones SNMP tienen que recibir paquetes en al menos 484 octetos de longitud
- Alguna implementación SNMP no corregirá o no manejará paquetes que excedan los 484 octetos
- Los *trap* asincrónicos son recibidos sobre el pórtico 162 del NMS
- UDP es más apropiado que TCP cuando ocurren frecuentemente cambios dinámicos de la ruta (por ejemplo, cuando hay problemas en la red)
- Los paquetes UDP minimizan las demandas localizadas en la red (los recursos no son paralizados como con el modo orientado a conexión)
- El agente y el NMS son los responsables de la recuperación de errores

El siguiente diagrama muestra la arquitectura de transporte UDP

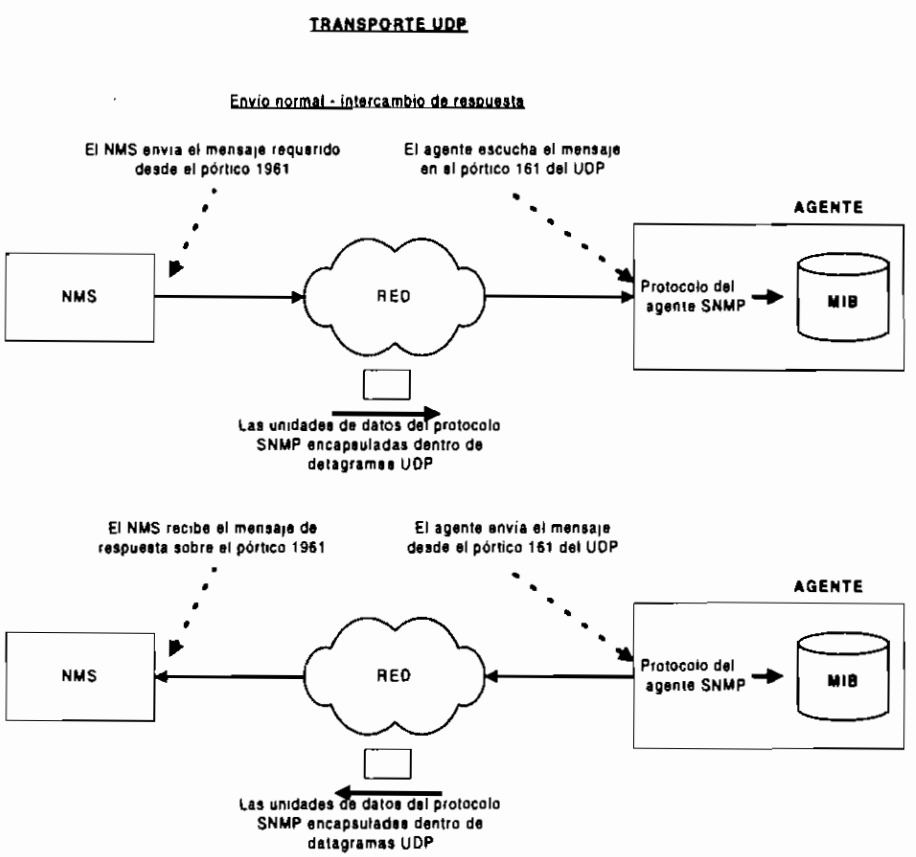


***Figura 3.61** Arquitectura de transporte UDP*

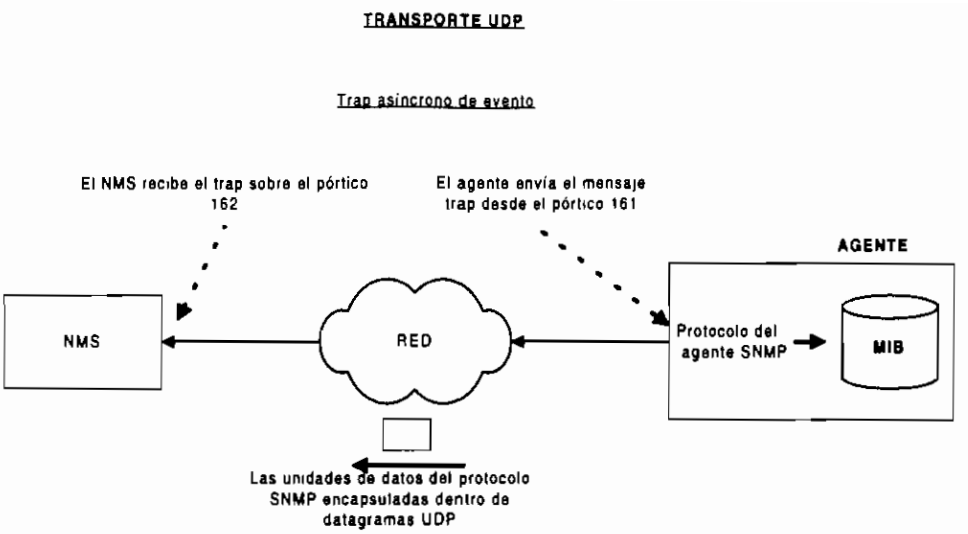


***Figura 3.62** Trap asincrónico de evento en el mecanismo de transporte UDP*

B. Protocolo SNMPv2

Las principales innovaciones de SNMPv2 son: mejora de rendimiento, mejora de seguridad y la posibilidad de construir una jerarquía de administradores.

B.1 Mejora de rendimiento

El protocolo original SNMP incluye una regla que dice que si un requerimiento *Get* o *GetNext* excede el máximo tamaño del paquete, ninguna información será regresada a nadie. Para obtener toda la información, los administradores podrían requerir realizar un gran número de requerimientos consecutivos debido a que no pueden determinar el tamaño de los paquetes respuesta.

Para mejorar el rendimiento, SNMPv2 ha introducido el PDU *GetBulk*. Opuesto a *Get* y *GetNext*, la información del *GetBulk* siempre retorna con tanta información como sea posible. Si la información requerida excede el tamaño máximo de un paquete UDP, la información será truncada y solamente la parte apropiada del paquete será retornada.

B.2 Mejora de seguridad

El protocolo SNMP inicial no tiene características de seguridad excepto por un simple mecanismo que envuelve el intercambio de passwords (*community string*). SNMPv2 introdujo un mecanismo de seguridad basado en el uso de '*parties*' y 'contextos'. Las *parties* tienen alguna relación con las entidades del protocolo. La figura 3.63 muestra la mejora de seguridad utilizando *parties* y contextos.

En la figura 3.63, tres *parties* han sido configuradas en el sistema administrador (Pa1, Pa2, Pa3) y tres *parties* en el sistema agente (Pb1, Pb2, Pb3).

Para controlar el acceso a las varias partes de un MIB, SNMPv2 ha introducido el concepto de *contexto*. Cada contexto se refiere a una parte específica de un MIB.

En el gráfico los contextos C1 y C2 se refieren a 2 áreas en el MIB. Los contextos pueden ser sobrepuestos y configurables dinámicamente, lo que significa que los contextos pueden ser creados, borrados o modificados durante la fase de operación de la red.

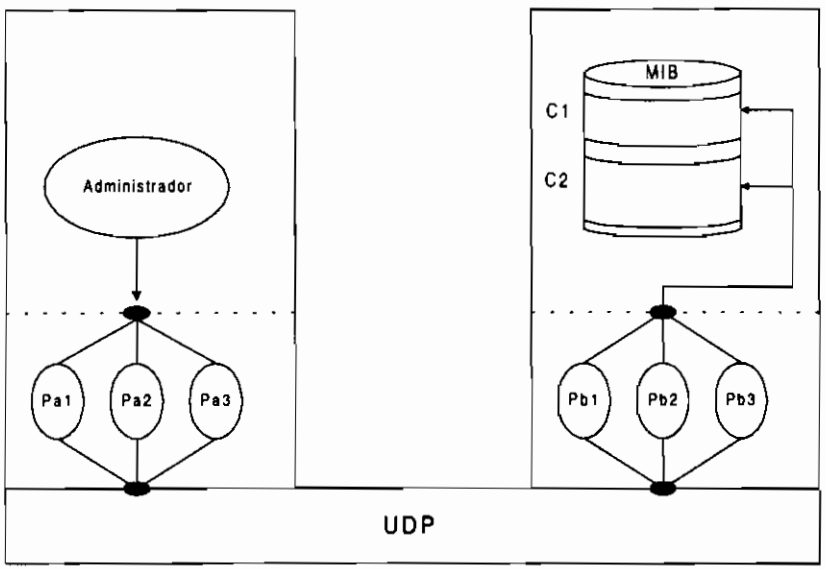


***Figura 3.63** Mecanismo de seguridad de SNMPv2 utilizando parties y contextos*

Para determinar qué *parties* son permitidas para realizar determinadas operaciones sobre qué partes del MIB, SNMPv2 tiene asociado con cada agente una *lista de control de acceso (ACL).*

B.3 Administración jerárquica

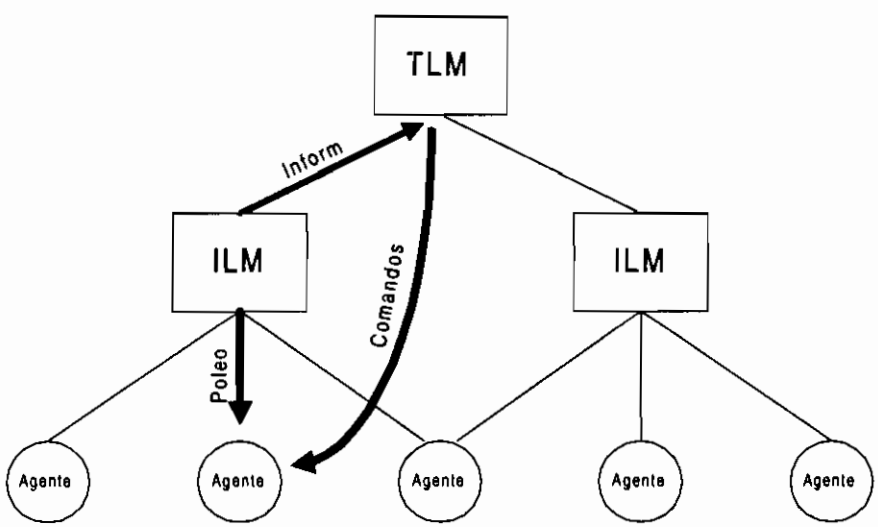


***Figura 3.64** Administradores de nivel intermedio en SNMPv2*

La experiencia práctica con el protocolo original SNMP mostró que en muchos casos los administradores eran incapaces de administrar más que unos pocos cientos de sistemas agentes. La causa para esta restricción es que SNMP realiza funciones de *poleo (polling)*. Para resolver este problema, SNMPv2 introdujo la idea de administradores de nivel intermedio (ILM). El poleo es ahora realizado por un número de administradores intermedios, que a su vez están bajo el control de un administrador de máximo nivel *(TLM-Top Level Manager)*, dividiendo de esta forma las funciones de poleo.

En el caso de que un administrador de nivel intermedio detecte en un agente en particular, un evento del cual el administrador máximo desea ser informado, un PDU especial (*Inform*) es generado. Luego de la recepción de este PDU, el administrador del máximo nivel opera directamente sobre el agente que causó el evento.

C. MIB (Management Information Base)

Las bases de información de administración (MIBs) son una colección de definiciones, las cuales establecen las propiedades del objeto administrado dentro del dispositivo a ser administrado. Cada dispositivo administrado guarda una base de datos de labores para cada una de las definiciones escritas en el MIB. Esta no es la base de datos actual, es dependiente de la implementación. Para identificar todas las variables que pueden ser administradas, un gran número de estándares MIB han sido desarrollados. Un estándar especial existe definiendo cómo describir las variables MIB. Este estándar es llamado *Structure of Management Information*. La definición del MIB es conforme a la provista por el SMI dado en el RFC 1155. La última MIB de Internet está dada en RFC 1213 algunas veces llamada MIB II.

Los criterios y la filosofía para las MIB estandarizadas son:

- Los objetos deben tener un único nombre
- Los objetos tienen que ser esenciales
- La estructura abstracta de la MIB necesita ser universal
- El estándar MIB mantiene solamente un pequeño número de objetos
- Se permiten extensiones privadas
- Los objetos deben ser generales y no muy dependientes del dispositivo
- Si el agente no administrable con SNMP entonces es mandatorio implementar el MIB Internet (actualmente dado como MIB-II en RFC 1157)

C.1 Nombrando un objeto

- Identificación universal no ambigua de objetos arbitrarios
- Pueden ser archivados utilizando un árbol jerárquico
- Están basados en esquema de identificación de objetos definidos por OSI

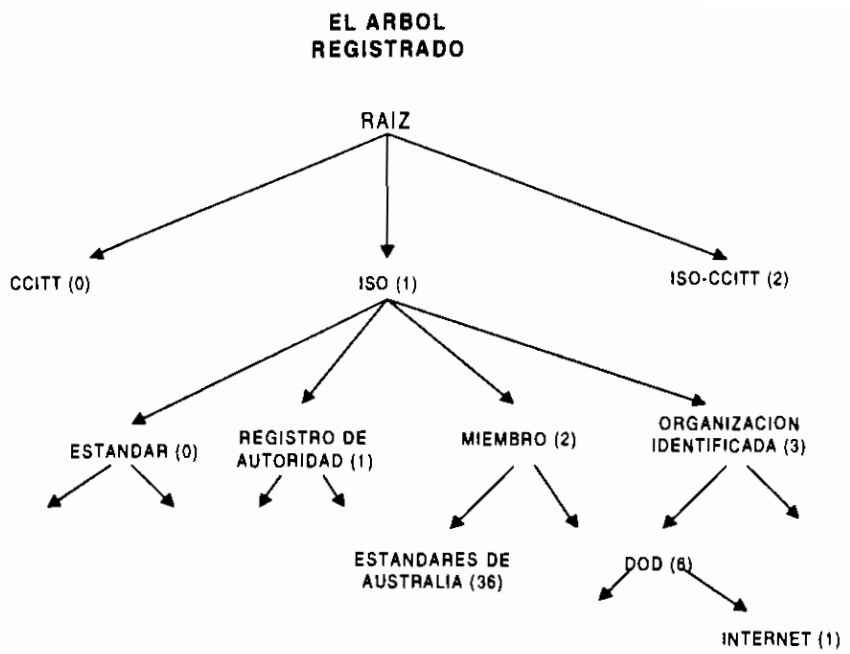


***Figura 3.65** Arbol registrado de nombres en SNMP*

C.2 Identificadores de objeto

- El nombre del objeto está dado por su nombre en el árbol
- Todos los nodos hijo tienen asignados valores enteros únicos dentro de ese nuevo sub árbol
- Los hijos pueden ser padres de más sub-árboles hijos (es decir, ellos son subordinados) donde el esquema numerado es aplicado recursivamente
- El objeto identificador (o nombre) de un objeto es la secuencia de valores enteros no negativos atravesando el árbol al nodo requerido
- La localización de un valor entero para un nodo en el árbol es un acto de registro por quien tenga autoridad delegada sobre ese sub-árbol
- Este proceso puede tener un número arbitrario de subniveles
- Si un nodo tiene un hijo entonces aquel es un nodo agregado
- Los hijos del mismo padre no pueden tener el mismo valor entero

D. RMON (Remote Monitoring)

Las redes de la actualidad soportan nuevas arquitecturas distribuidas, aplicaciones de alto rendimiento, y grandes poblaciones de usuarios que tienen un impacto significativo sobre la efectividad de las soluciones de gestión de redes y requieren estándares de red que guarden las ventajas de la tecnología de conectividad.

SNMP es un protocolo de administración de red ampliamente implementado, que utiliza un *software* de agente dentro de dispositivos de red que recogen información y estadísticas del tráfico. Los agentes reciben constantemente datos que son grabados en las tablas MIB. Los administradores de red pueden obtener

información haciendo requerimientos de envío a los MIB de los agentes, en un proceso llamado *POLLING*.

Si bien los contadores MIB graban estadísticas agregadas, ellos no proveen ningún análisis histórico del tráfico diario. Para compilar una vista comprensiva del flujo de tráfico diario y de sus tasas de cambio, los administradores deben polear a los agentes SNMP continuamente, cada minuto de cada día. De esta forma, los administradores pueden usar SNMP para evaluar el rendimiento de la red y descubrir tendencias de tráfico, tales como segmentos que están próximos a tener un tráfico corrupto. La ventaja de SNMP es que pueden deshabilitarse pórticos automáticamente (por programación) o tomar acciones correctivas en reacción a los datos de red históricos.

Sin embargo, las desventajas del *polling* de SNMP se presentan así:

- En redes grandes, el *polling* genera tráfico substancial de administración de red, contribuyendo a problemas de congestión.
- Las estaciones de administración que pueden ser fácilmente recolectoras de información de 8 segmentos, podrían no ser capaces de guardar monitoreo de 48 segmentos.

El MIB RMON fue publicado en noviembre de 1991 por el IETF (*Internet Engineering Task Force*) para sobrellevar las limitaciones de SNMP en redes crecientes distribuidas. El propósito de MIB RMON es permitir a SNMP monitorear dispositivos remotos más eficiente y proactivamente[42].

El MIB RMON consiste de un grupo de datos estadísticos, analíticos y de diagnóstico que pueden ser mostrados usando herramientas estándar a través de líneas de productos multivendedor, proveyendo de esta manera análisis remoto de la red independiente del vendedor. La combinación de *probes* RMON y *software* de cliente RMON implementan RMON en el ambiente de la red. La clave para la efectividad del monitoreo de RMON es su habilidad para almacenar la historia de los datos estadísticos en el *probe*, removiendo de esta manera la necesidad de realizar un "poleo" continuo para construir una vista de las tendencias de la red.

Los probes RMON no destructivos dispersos a lo largo de los segmentos LAN trabajan autónomamente y reportan cuando un evento de red excepcional ocurre. Las capacidades de filtración del *probe*, permiten capturar tipos específicos de datos basados en parámetros definidos por el usuario.

RMON dedicado y distribuido

Los agentes RMON pueden ser implementados solitariamente, con *probes* dedicados, cada uno de los cuales monitorea un único segmento LAN. Sin embargo, mientras el monitoreo de la red de un segmento a la vez es de algún uso del segmento, esto decrementa el propósito de RMON. Para administrar

[42] El término proactivamente, intenta hacer referencia a la capacidad de manejar funciones en forma dinámica e "inteligente", es decir, no en función de un poleo constante, sino en función de las necesidades (de informar al administrador) que vayan presentándose.

proactivamente una red con RMON se requiere que todos los segmentos sean monitoreados a la vez. Dependiendo del tamaño de la red, el costo de emplear *probes* RMON a lo largo de todos los segmentos LAN puede ser substancial. Una alternativa a utilizar *probes* dedicados es mover los *probes* físicamente desde segmento a segmento para ganar una perspectiva amplia del sistema sobre patrones de tráfico de la red. Sin embargo este proceso es dificultoso y consume tiempo.

El RMON distribuido monitorea la actividad de paquetes y correlaciona el estado y estadísticas de rendimiento desde múltiples segmentos de LAN remotos, permitiendo a los administradores de red ver como los cambios de topología afectan la red ampliada.

RMON distribuido a través de grupos de trabajo es la forma más efectiva de tomar ventaja de la funcionabilidad de RMON debido a que comprende el ahorro de RMON dedicado.

El estándar RMON II es un estándar propuesto por la industria que permite a los administradores de red monitorear la red hasta el nivel de aplicaciones del *stack* de protocolos de red. Así, además de monitorear el tráfico de la red y su capacidad, RMON II provee información sobre la cantidad de ancho de banda de red usado por aplicaciones individuales, un factor crítico cuando se trata de resolver problemas en ambientes de red cliente/servidor.

Mientras que RMON busca problemas físicos sobre la red, RMON II toma una vista de un nivel más alto. Aquel monitorea patrones actuales del uso de la red. Mientras un *probe* RMON mira el flujo de paquetes de un ruteador a otro, RMON II mira cual servidor envía el paquete, cual usuario está destinado a recibirlo, y que aplicación representa ese paquete. Los administradores de red pueden usar esta información para segregar usuarios por su ancho de banda de aplicación y requerimientos de tiempo de respuesta.

RMON II no es un reemplazo para RMON pero sí es una tecnología complementaria. RMON II provee un nuevo nivel de diagnóstico y monitoreo que es construido sobre RMON.

En redes cliente/servidor, los probes RMON II bien localizados pueden ver las conversaciones de aplicaciones para la red entera. Buenas localizaciones para los probes RMON II son en centros de datos o conmutadores de grupo de trabajo, o en servidores de alto rendimiento en el *farm* de servidores[43]. La razón es simple, por aquí pasa la mayoría de aplicaciones. Los problemas físicos ocurren más comúnmente sobre el nivel de grupo de trabajo, donde los usuarios ingresan a la red. Así, el grupo de trabajo es donde las implementaciones RMON son más útiles y de mayor costo efectivo.

[43] El término *farm* de servidores se utiliza generalmente para hacer referencia a un grupo de servidores que se encuentran en una misma habitación, y que se conectan al mismo dispositivo de conectividad.

3.5.3 ESQUEMA DE ADMINISTRACIÓN DE UNA RED ESTRUCTURADA DE DATOS

En el mundo de hoy, cualquier implementación debe satisfacer las necesidades de los negocios asociados a ellas. Las implementaciones deben resolver un problema de negocios o incrementar la eficiencia de los métodos actuales de cumplimiento de trabajo mientras se reducen costos.

Es importante aclarar que una forma de ahorrar dinero a una organización es tratar de automatizar los sistemas al máximo. Existen 4 niveles de actividad que se debe entender antes de aplicar administración a un servicio o dispositivo:

- *Inactivo,* cuando no se monitorea y se ignora que se recibió una alarma
- *Reactivo,* cuando se reacciona a un problema después de que éste ha ocurrido pero el monitoreo no ha sido aplicado
- *Interactivo,* cuando se monitorea componentes pero debe ir buscándose la solución eliminando las posibles causas hasta llegar a la raíz de la que generó la alarma
- *Proactiva,* cuando se monitorea componentes y el sistema provee una alarma de la raíz del problema, manejándola y restaurándola lo más pronto posible

Estos 4 niveles de actividades son muy comunes en las organizaciones de soporte. Estas actividades son cumplidas por grupos con diferentes metas y enfoques (soporte de escritorio, soporte de red, soporte de sistemas, etc).

Un grupo importante en una organización de soporte es el de *Help desk*, los cuales son la primera línea de comunicación entre los usuarios finales y la organización de soporte. Este grupo debe entender claramente a quien recurrir dependiendo del problema que se presente. Este grupo difícilmente es en la actualidad totalmente automatizado, y por tanto representa porcentaje de tiempo significativo en la solución de problemas.

La organización de soporte debe encargarse de realizar reportes de los análisis de tendencias. Un análisis de tendencia es usualmente una función local que busca tasas de crecimiento sobre *hardware* local, aplicaciones y sistemas. El personal que se recomienda para realizar esta tarea es gente que actualmente esté familiarizada con el ambiente de la empresa, y que genere los reportes en términos que el personal de soporte local pueda entender.

Dentro de este último análisis es importante que se vaya midiendo el desempeño de las partes analizadas. Un buen parámetro de medición es la disponibilidad, la que puede ser calculada con la siguiente fórmula:

$$\text{Disponibilidad} = 1 - \frac{\text{\# minutos de funcionamiento}}{(10080 \text{ minutos/semana} - \text{\# minutos de malfuncionamiento})}$$

Esta fórmula daría la disponibilidad por dispositivo, y debe tenerse cuidado de mezclas con otros dispositivos y tratar de obtener la disponibilidad de un sistema basándose en esto.

Otro método para calcular la disponibilidad, es obtener una lista de servicios, provistos en la red, por prioridad. El reporte de la disponibilidad de cada uno de los servicios sobre una base mensual. Debe utilizarse un modificador o un parámetro de peso sobre esos servicios que son considerados más importantes a la organización. La siguiente fórmula especifica la disponibilidad de los servicios de acuerdo a un peso de importancia:

$$\text{Disponibilidad} = 1 - \frac{\text{\# minutos de funcionamiento} * \text{Factor de peso}}{(10080 \text{ minutos/semana} - \text{\# minutos de malfuncionamiento})}$$

El tiempo de respuesta asociado con los servicios de red específicos es importante al nivel de servicio que el usuario final recibe.

En ambientes LAN el monitoreo de la utilización actual, la utilización de *buffers* y su tiempo de respuesta relacionada, dan un cuadro informativo de la utilización actual de una interfaz. Algunos dispositivos RMON pueden proveer estadísticas sobre la espera de paquetes entre 2 nodos sobre la red. Adicionalmente, algunas aplicaciones tienen auditores asociados que permiten monitorear su rendimiento y tiempo de respuesta (ej: Oracle, Sybase, Informix).

Cuando se están definiendo criterios que al ser cumplidos activen una alarma, debe considerarse la correlación que busque una causa común y que permita fácilmente definir cual es la causa raíz del problema que generó la alarma. Por ejemplo, supongamos que se tienen 3 estaciones de trabajo conectadas a un *hub*, y supongamos que en el *hub* se produce una falla. Se generarán entonces cuatro alarmas, tres de ellas procedentes de las estaciones informando que tienen problemas en la comunicación con el resto, y una procedente del *hub* que informa tener problemas. La única alarma que interesa es la alarma proveniente de la causa raíz (la del *hub*) y no las alarmas de efecto secundario (las de estaciones). Por esto debe definirse bien la correlación entre la causa raíz de un problema y los efectos secundarios que pueden generar alarmas, para que ésta funcione con mayor eficiencia.

Cuando el flujo de proceso de trabajo actual es documentado, se puede ver fácilmente que los procesos claves pueden ser manejados por el grupo *Help desk*. La clave del éxito en la operación de la organización de soporte (departamento de administración de sistemas de datos) no está en contratar un gran grupo de "caros" ingenieros de alto nivel para que cumplan el trabajo. La gente es motivada cuando ellos son empleados y entrenados en la organización. La construcción de una base de conocimientos de síntomas y las tareas asociadas con la detección y corrección de esos problemas pueden realizarse con el uso del buen sentido común. Por el proceso de eliminación, una lista de causas probables puede ser encontrada.

Construir la base de conocimientos e irla desarrollando en la organización hará que nuevo personal sea más productivo.

Para poder realizar el seguimiento de un problema que se haya presentado y de su solución (y quién lo está solucionando) es importante que se genere un reporte de problema, para poder estimar costos de mantenimiento y poder realimentar con la solución a la base de conocimientos.

En resumen, se podría plantear el esquema de administración de una red estructurada de datos como se muestra en la figura 3.66.

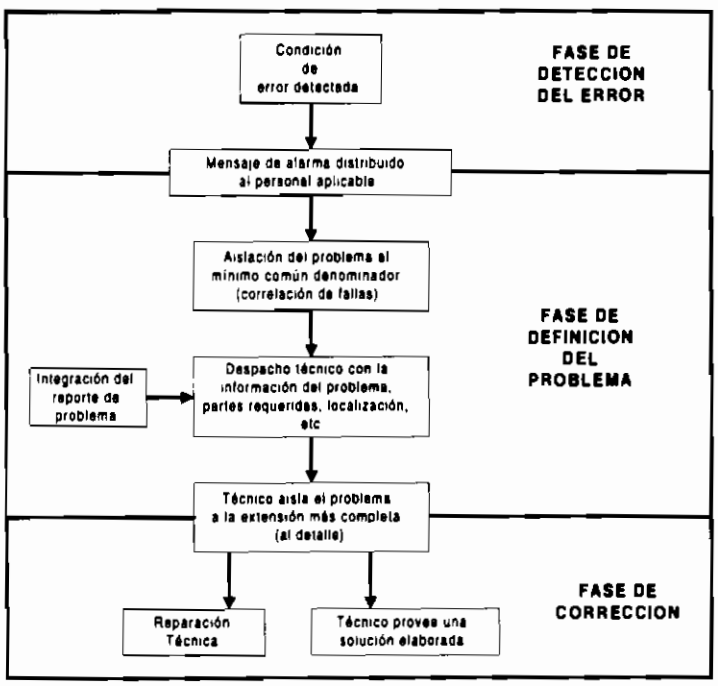


***Figura 3.66** Fases de administración de una red estructurada de datos*

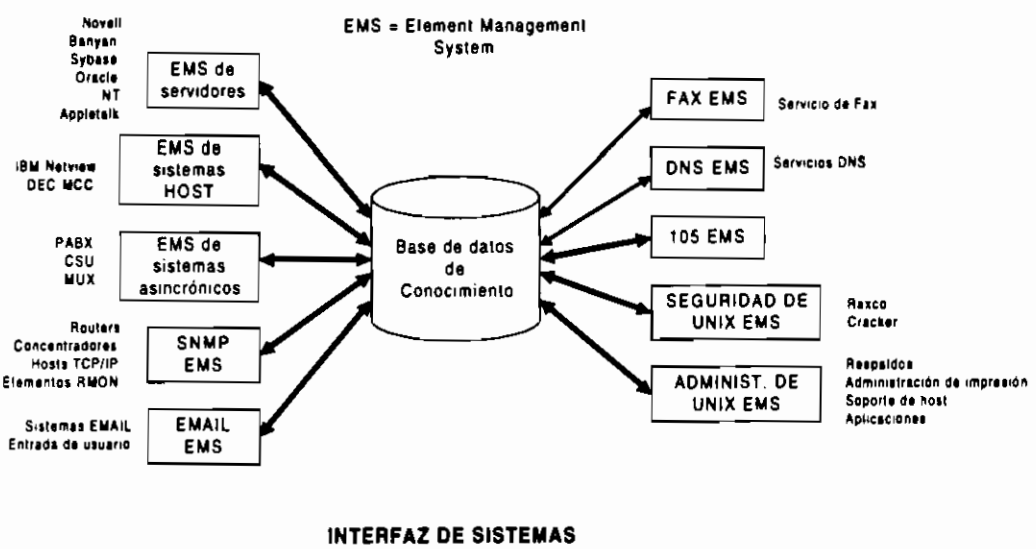


***Figura 3.67** Base de datos de conocimientos recogidas de problemas reportados por aplicaciones*

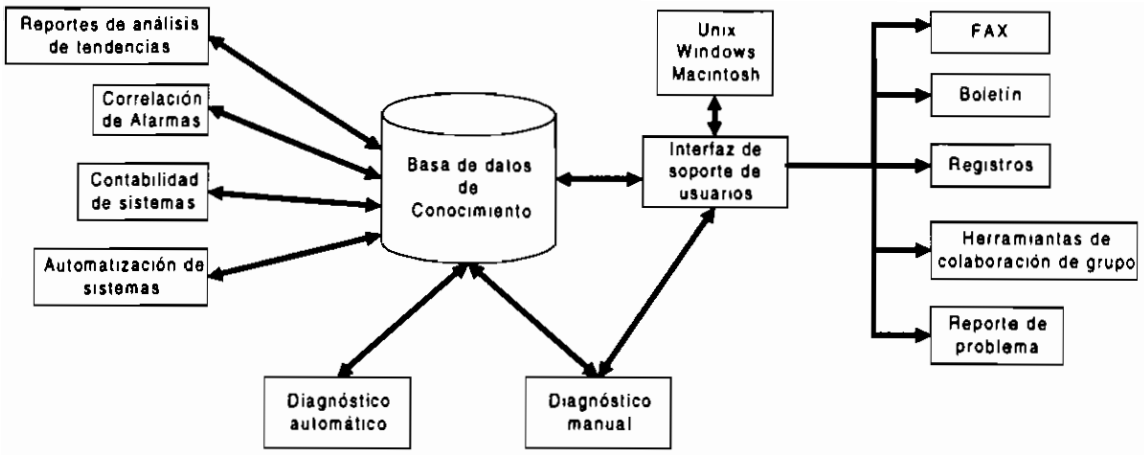


***Figura 3.68** Esquema general de administración*

Existe un gran número de excelentes productos disponibles que proveen capacidades para administrar tanto *hardware* como servicios y aplicaciones. La forma en que estos sistemas sean implementados es crítica en que cada capacidad de administración instalada debe satisfacer una necesidad de negocios para un sistema. Adicionalmente, estos diversos sistemas deben ser integrados juntos y dentro de organizaciones de soporte para alcanzar máxima efectividad.

Capítulo IV

Análisis y diseño de un subsistema de conectividad integrado sobre un sistema de cableado estructurado de una red hipotética de datos

IV. ANÁLISIS Y DISEÑO DE UN SUBSISTEMA DE CONECTIVIDAD INTEGRADO SOBRE UN SISTEMA DE CABLEADO ESTRUCTURADO DE UNA RED HIPOTÉTICA DE DATOS

En la búsqueda de métodos para el análisis y diseño de redes, se encontraron fundamentalmente dos métodos[44]:

- Planeación estratégica
- Fundamentos de diseño

a. Planeación estratégica

La planeación estratégica se define como el proceso de escoger objetivos a largo plazo y decidir acciones que permitan alcanzar estos objetivos. La planeación estratégica consta de dos etapas, cada una de las cuales se divide en 3 fases:

- Etapa I: Definición de los requerimientos
  - Fase 1: Estrategia
  - Fase 2: Factibilidad
  - Fase 3: Análisis
- Etapa II: Desarrollo de la red
  - Fase 1: Diseño
  - Fase 2: Implementación
  - Fase 3: Administración

Durante la primera etapa de la planificación estratégica, se define si el proyecto debe o no realizarse. Una vez definidos algunos parámetros cualitativos y de requerimientos de la red durante la fase de estrategia, se realiza una cuantificación aproximada de los costos que permitirían llevar a cabo el proyecto y se realiza un análisis de factibilidad. Dependiendo de la respuesta que se obtenga de la fase de factibilidad se continúa o se detiene el proyecto.

Si se decide continuar con el proyecto, se continúa con la fase 3 de la etapa I, donde se realiza una cuantificación detallada de los requerimientos especificados en la fase de estrategia.

Posteriormente se dará paso a la segunda etapa: desarrollo de la red. En la primera fase de esta etapa, se obtiene la configuración de la red, partiendo de los resultados obtenidos en la fase de análisis. La fase de implementación es poner en práctica la fase de diseño. En la fase de administración de red se definen estándares,

[44] Información recopilada del documento titulado "Evaluación de metodologías de diseño de redes" (por: Iván Cuéllar) de la Universidad de los Andes en Colombia. Documento disponible en Internet (http://ainsuca.uniandes.edu.co/tesis/evaluaci.htm).

herramientas y procedimientos que aseguran una correcta utilización y mantenimiento de la red.

b. Fundamentos de diseño

Este es un método práctico para la implementación de redes nuevas o mejoramiento de las actuales, determinando los elementos básicos para su diseño. Consta de los siguientes pasos:

- Estudio de factibilidad
- Preparación de un plan de diseño de la red
- Entendimiento de la red actual (si la hay)
- Definición de los nuevos requerimientos
- Identificación del alcance geográfico
- Análisis de los mensajes (promedio y pico)
- Cálculo del tráfico de red
- Identificación de la seguridad requerida
- Diseño de la configuración de la red
- Evaluación de los protocolos a emplear
- Evaluación de las alternativas de *hardware*
- Cálculo del costo
- Implementación

En este método, durante el estudio de factibilidad se intenta definir el problema que se está atacando y no la factibilidad misma del proyecto. Los pasos posteriores se describen por sí solos.

Método utilizado en la presente tesis

Con el fin de relacionar el análisis y diseño seguidos en esta tesis, con la planificación estratégica y el método de fundamentos de diseño de redes propuesto en este capítulo, se presenta la Tabla 4.1 para comparación de los métodos.

En función de los dos métodos de análisis y diseño de redes antes descritos, y considerando el temario y alcances propuestos, se puntualiza lo siguiente:

- El alcance y temario propuestos pueden ajustarse a cualquiera de los dos métodos de análisis y diseño de redes, aunque se adapta de mejor manera al método de fundamentos de diseño de redes
- Puede plantearse un método propio de análisis y diseño de redes

Debido a que los métodos de análisis y diseño de redes mencionados, son métodos sugeridos y no obligatorios, en el presente capítulo se desarrollará el análisis y diseño de la red planteada, siguiendo una lógica similar al método de fundamentos de diseño de redes. Debe aclararse que la selección de uno de los métodos debe realizarse principalmente en función de la envergadura y alcance del proyecto en estudio, ya que al

tratarse de un proyecto grande (en tiempo) es recomendable utilizar planeación estratégica.

Análisis y diseño de la red planteada en esta tesis	**Planificación estratégica de redes**	**Fundamentos de diseño de redes**
4.1 Análisis de la implementación actual de la red hipotética de datos	Etapa I: Definición de los requerimientos • Fase 1: Estrategia • Fase 2: Factibilidad • Fase 3: Análisis	• Estudio de factibilidad • Preparación de un plan de diseño de la red • Entendimiento de la red actual (si la hay) • Definición de los nuevos requerimientos • Identificación del alcance geográfico • Análisis de los mensajes (promedio y pico) • Cálculo del tráfico de red • Identificación de la seguridad requerida
4.2 Criterios de diseño y normas	Etapa II: Desarrollo de la red • Fase 1: Diseño	• Diseño de la configuración de la red • Evaluación de los protocolos a emplear
4.3 Alternativas de un subsistema de conectividad de una red de datos para su integración sobre un sistema de cableado estructurado y parámetros que guían a la mejor selección técnica	• Fase 2: Implementación	• Evaluación de las alternativas de *hardware*
4.4 Características y especificaciones técnicas de los elementos del subsistema de conectividad seleccionado		
4.5 Aplicaciones factibles de implementar sobre el sistema planteado	• Fase 3: Administración	
5. Análisis de inversión		• Cálculo del costo • Implementación[45]

***Tabla 4.1* Comparación entre los temas de análisis y diseño de redes a desarrollar en los capítulos 4 y 5 de esta tesis, con el método de planeación estratégica de redes y el método de fundamentos de diseño de redes**

Se eligió como guía el método de fundamentos de diseño, ya que el análisis de la red planteada, a pesar de que puede considerarse como un proyecto de alta envergadura (1 año en tiempo aproximadamente), parte de este proyecto (sobre la infraestructura de transporte) ya fue analizado, en tanto que la parte correspondiente al subsistema de conectividad no tiene su estudio pertinente, y por motivos de desarrollo del presente y siguientes capítulos se asume que su factibilidad es dable. Siendo la característica más importante del modelo de planeación estratégica, la determinación de factibilidad de un

[45] La implementación no se llevará a cabo pues no está dentro del alcance de esta tesis

proyecto en su etapa inicial, en esta tesis esa característica se vería opaca, pues se ha asumido que el proyecto es factible de realizar. Esta es la razón principal para no elegir el método de planeación estratégica en esta tesis.

En la Tabla 4.1 se puede ver que existe coincidencia en el orden en el que se realizará el análisis y diseño de la red que se plantee con el método fundamentos de diseño, con excepción de los numerales 4.4 y 4.5, en los que se evaluarían las características y especificaciones técnicas de los elementos del subsistema de conectividad seleccionado y las aplicaciones factibles de implementar sobre el sistema planteado respectivamente.

El numeral 4.4, se desarrollará tratando de describir detalladamente, las características que deberían tener los elementos de la red solución seleccionada, pudiendo considerarse este numeral como complementario al 4.3.

En el numeral 4.5, referente a las aplicaciones factibles de implementar, se tratarán determinadas aplicaciones que deben ser planteadas como requerimientos en el numeral 4.1, pero desde un punto de vista ya no de requerimiento, sino de beneficios que pueden brindar esas aplicaciones, es decir como un justificativo a la inversión a realizar.

4.1 ANÁLISIS DE LA IMPLEMENTACIÓN ACTUAL DE LA RED HIPOTÉTICA DE DATOS

En la práctica, normalmente los diseñadores de redes se encuentran fundamentalmente con dos situaciones de alternativas de diseño:

- Diseño de una red de datos totalmente nueva
- Diseño de una red que fue implementada anteriormente (rediseño o actualización)

En cualquiera de los dos casos, las alternativas de diseño podrán ser de lo más variadas y tan simples o complicadas y sofisticadas como se desee. Sin embargo, el factor que limitará y definirá qué alternativa escoger será la capacidad económica.

Por esta razón es tan importante se realice un análisis de la relación costo/beneficio en cualquier diseño sugerido antes de su implementación.

En este capítulo se va a suponer el análisis de una red existente que se encuentra en funcionamiento en una institución bancaria del país, cuyo nombre se va a omitir. Será entonces el análisis de una red real. No se ha escogido el diseño de una red totalmente nueva, pues es un caso más sencillo que el que se va a exponer en este capítulo. Además, entre las alternativas de diseño que se propondrán, estará una que involucre un rediseño total de la red actual, lo que es un caso muy parecido al del diseño de una red de datos totalmente nueva.

4.1.1 EVOLUCIÓN DE LA RED HIPOTÉTICA DE DATOS

Como normalmente hasta no hace mucho tiempo sucedía en nuestro medio, el crecimiento y evolución de las redes se realizaba en función de una planificación a corto plazo y respondiendo en la mayoría de los casos a una necesidad mediata o inmediata.

Es así, que la red hipotética motivo de este estudio, se inició como una pequeña LAN *Token-Ring* aislada, utilizando cable STP y como dispositivos de concentración de cableado los MAU en una topología física de estrella hacia las estaciones y en anillo entre MAUs, y una topología lógica en anillo. El método de acceso al medio era de paso de testigo (*token*).

Esta red, inicialmente servía para prestar algunos servicios de red tales como: servicios de impresión y servicios de archivos principalmente. Un servicio importante que se obtenía de esta red, era la conexión a un *host* IBM en el que se realizaban muchas tareas relacionadas con la entidad hipotética.

La comunicación con el *host* se realizaba desde terminales en un ambiente distribuido utilizando el *stack* de protocolos SNA. Sin embargo, es posible realizar la conexión al *host* desde cualquier computador conectado al segmento de red a través de un *gateway* que permite realizar el paso de un protocolo típico de LAN (IPX, IP) hacia SNA (ver fig. 4,1).

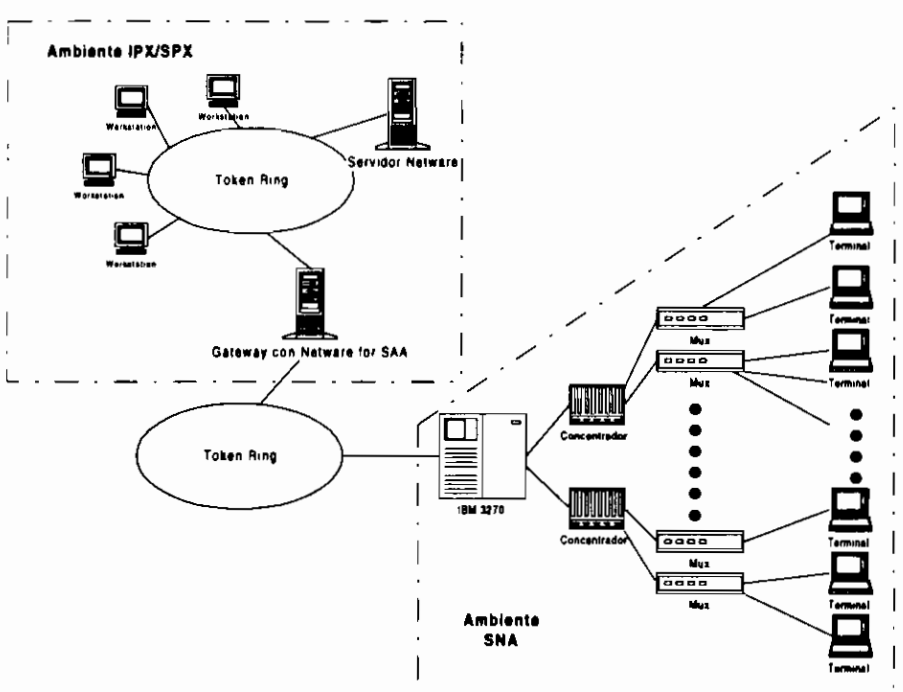


***Figura 4.1* Configuración inicial de la red hipotética de datos**

Una vez que se analizaron las ventajas de mantener computadores que realicen emulación al *host* y a la vez permitan realizar otras funciones en otros ambientes (por ejemplo: DOS, WINDOWS), mediante el uso de procesadores de texto y hojas

electrónicas, además de la compartición de archivos e impresoras, más LANs fueron implementadas y poco a poco las terminales "tontas" de conexión directa al *host* fueron desplazadas.

La interconexión de las LANs que trabajaban en un ambiente IPX se realizaba colocando en los servidores dos tarjetas de red, de manera que se tengan las LANs *Token-Ring* segmentadas entre sí. Poco a poco el ambiente SNA que era el más difundido inicialmente se redujo al *mainframe* principal con las aplicaciones que contenía, y la mayor parte se convirtió en un ambiente IPX/SPX con Netware, como se muestra en la figura 4.2:

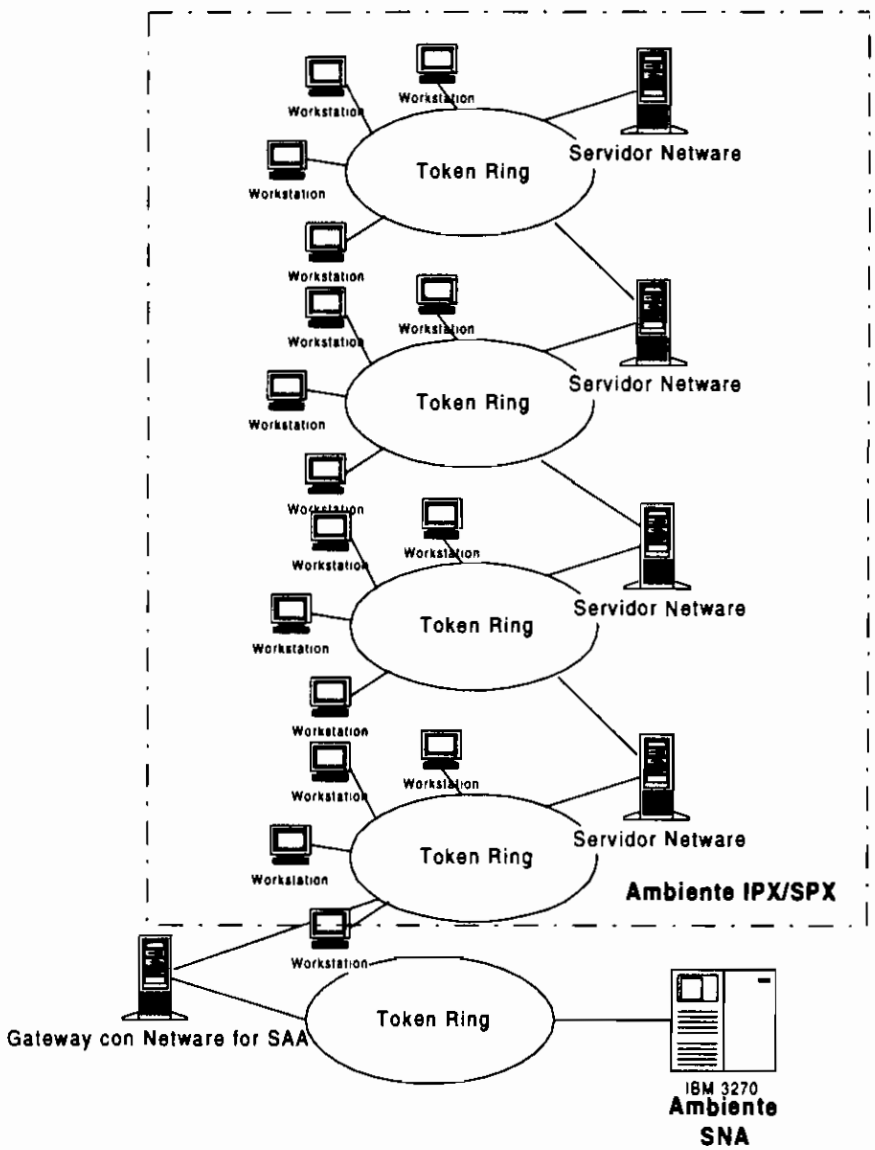


***Figura 4.2** Configuración intermedia de la red hipotética de datos*

4.1.1.1 Problemas que se presentaron

La red se podía controlar y funcionaba de manera adecuada hasta cuando se presentaron los siguientes problemas principalmente:

- *Las estaciones de las LANs perdían conexión con el servidor fruto de fallas en los MAUs*

Este problema se debía principalmente a que los MAUs eran dispositivos que funcionaban con pequeños relés, es decir poseían dispositivos electromecánicos que son más sensibles de desgaste con el tiempo. Esto podía solucionarse haciendo la adquisición de dispositivos netamente electrónicos. Debía considerarse adicionalmente que el cambio a dispositivos electrónicos (especialmente si se tendía a lo que empezaba a crecer tecnológicamente en popularidad y a precios bajos, las redes *Ethernet*), involucraba seguramente el cambio de cableado, pues el cable STP tipo 1 utilizado, era muy grueso, difícil de manejar y no estaba diseñado para conectores RJ45 que era lo que recomendaban los estándares.

- *La administración de los servidores y MAUs era complicada debido a su ubicación física*

Este problema se presentaba cuando se requería la manipulación directa del servidor o de alguno de los MAU, debido a que estos dispositivos se encontraban distribuidos por pisos en la entidad. Es decir, cada servidor ocupaba el piso al que servía en su red, y los MAU se encontraban repartidos a lo largo de cada piso formando su anillo. Una molestia típica que se presentaba era cuando se requería "resetear" cada uno de los MAU, se tenía que ir a lo largo de todo el piso en busca de cada MAU para irlo reseteando debido a que no se encontraban concentrados en un solo sitio. Situación similar ocurría con los servidores de piso, además de que la seguridad de éstos no era la más óptima.

- *Surge la necesidad de que usuarios de un determinado anillo utilicen los servicios prestados por servidores ubicados en otros anillos*

Mucha de la información que era procesada en un departamento, era la base de trabajo para el desarrollo de otro proceso en otro departamento, ubicado en cualquier parte de la entidad. Esto se debía principalmente a que se empezaba a realizar un trabajo ya no por funciones, sino por sistemas de procesos que involucraban a varias áreas. Es importante resaltar este último hecho, pues es muy difícil utilizar este modelo sin la infraestructura informática adecuada. El problema que se generaba en la red se reflejaba principalmente en el crecimiento de tráfico en los servidores que se encargaban de pasar información entre segmentos de redes, lo que en momentos se traducía en descensos del rendimiento de estos servidores.

- *El ambiente IPX/SPX no permitía la utilización de algunos servicios*

Internet y sus servicios se mostraron como una necesidad para los usuarios de la red de datos de la entidad hipotética.

- *Más usuarios requerían los servicios de red*

Se hacía necesaria la instalación de nuevos segmentos de red para nuevos usuarios.

4.1.1.2 Soluciones

El problema a enfrentar se resume en la ausencia de una red estructurada de datos. Si bien la red como tal podía haber dado el servicio que lo requerían los usuarios, los problemas se presentaban principalmente para la parte técnica responsable de esa red. Si se presentaba una falla, los tiempos de respuesta en la recuperación de la falla no podían ser lo más óptimos, pues la red no estaba bien organizada, la red era difícil de administrar.

Adicionalmente, la influencia de dispositivos que empezaban a dar fallas, agravaba la situación.

Antes de seguir instalando nuevas redes, debían tomarse medidas correctivas.

Para enfrentar este problema, se propusieron las siguientes acciones a tomar como parte de una solución a corto plazo:

- Adquisición de *hubs Ethernet* (electrónicos para conectores RJ45 y más económicos que los *Token-Ring*) para las nuevas redes que vayan a instalarse. Los *hubs* serían agrupados por pisos, y estarían juntos en un sitio adecuado y seguro. Esto implicaba que para las estaciones de trabajo se debía hacer la adquisición de tarjetas de interfaz de red *Ethernet*.
- Adquisición de *hubs Token-Ring* (electrónicos para conectores RJ45) que irían en reemplazo de los ya obsoletos MAUs de los segmentos de red ya existentes. Esto implicaba el tendido de cableado UTP en lugar del anterior STP en las redes existentes, pero las tarjetas de interfaz de red podían mantenerse las mismas ya que poseían los 2 tipos de conectorización (DB9 y RJ45). Los *hubs* serían agrupados por pisos, y estarían juntos en un sitio adecuado y seguro.
- Agrupación de los servidores de red en el centro de cómputo, para lograr una mejor administración y seguridad (puede sonar redundante pues parte de la administración está en garantizar la seguridad).
- Tendido de cableado UTP para todos los segmentos de red: nuevos y existentes.
- Adquisición de un ruteador que se encargue de conectar todos los segmentos de red, liberando de esta función a los servidores de red.
- Implementación del *stack* de protocolos TCP/IP, con el objeto de poder acceder a los servicios de Internet desde cualquier estación de la red LAN.

Paralelamente, y como una solución definitiva para largo plazo, se iniciaba la contratación de personas con experiencia para que realicen el estudio de factibilidad de implementación de cableado estructurado para la entidad.

4.1.1.3 Resultados

De las medidas a tomar como una solución a corto plazo, se obtuvieron los siguientes resultados:

- Mayor estabilidad de la red debido a la eliminación de dispositivos electromecánicos
- La implementación de un *backbone* colapsado al ruteador, liberó a los servidores de red de funciones de ruteo
- Se mejoró la administración tanto de servidores como de equipos de conectividad (*hubs Ethernet* y *Token-Ring*). Sin embargo, todavía se presentaban dificultades cuando se realizaban modificaciones o adiciones, pues no se contaba con un modelo estructurado, ya que el cableado de tendido horizontal se conectaba directamente entre el equipo terminal de usuario y el equipo activo de conectividad (*hubs*), y no a través de rosetas ni paneles de distribución (*patch panels*). Adicionalmente, no se contaba con la implementación de ningún protocolo de administración de red.
- La implementación del *stack* de protocolos TCP/IP, condujo a la adquisición de *software* que permita la traduccción de direcciones, de tal forma de mantener una red interna IP dentro de la entidad hipotética, y estar en la capacidad de manejar las direcciones externas de la red Internet.

Del estudio de factibilidad para implementar un sistema de cableado estructurado, como una solución definitiva a mediano plazo, se obtuvieron los siguientes resultados:

- Se requerían 1650 salidas de telecomunicaciones para satisfacer las necesidades de ese momento, de las cuales: 785 eran destinados para datos, 757 para voz, 34 para CCTV y 74 para control.
- Con el objeto de calcular la demanda final, se consideraron los siguientes parámetros: factor de crecimiento relativamente bajo (2%), factor de utilización inicial promedio del 0,7 y un factor de utilización final del 0,9.
- De los puntos anteriores se resume en la Tabla 4.2 el sistema de datos que interesa estudiar en la presente tesis.
- Para el subsistema de conectividad se planteó la utilización redes *Ethernet* 10BaseT conmutadas y compartidas en las redes horizontales de piso. Para la vertical se recomendó la utilización de *Fast Ethernet* o ATM (mínimo a 100 Mbps). Los servidores se conectarán a un segmento funcionando a 100 Mbps.
- El subsistema de conectividad contará entonces (concluyendo del punto anterior) con un *switch* principal que tendrá funciones de ruteo con un *backplane* que maneje 100 Mbps como mínimo, y con *switches* secundarios

para cada piso sirviendo conexiones 10BaseT conmutadas o compartidas. Los *switches* secundarios se conectarán al *switch* principal a través del cableado de tendido vertical con interfaces de 100 Mbps mínimo.

Cálculo de la vertical de datos	
Número de pisos	10
Número de fibras ópticas por piso	6
Cantidad de fibras ópticas	60
Conectores ST para patch panel de fibra	*60*
Número de patch panels de fibra de 24 ST (MDF)	*3*
Número de patch panels de fibra de 6 ST (SDF)	*10*
Cálculo de la horizontal de datos	
Demanda inicial Do	785
Factor de crecimiento F	2 %
Demanda final a 10 años Df=Do(1+F)^10	953.3
Grado de utilización futura GUT	0.9
Puertos UTP categoría 5 Df/GUT	1059.1
Cantidad de patch panels de 24 puertos (SDF)	*46*

***Tabla 4.2** Resultados obtenidos de un estudio inicial de cableado estructurado para la parte de datos de la red hipotética en estudio*

- Los equipos a adquirirse deberán contar con funciones de administración y monitoreo (SNMP).
- Los equipos activos deberán poseer fuentes de alimentación redundante, características de modularidad y permitirán el cambio o adición de módulos sin necesidad de apagar el sistema, es decir con el equipo encendido.
- Se estableció un tiempo aproximado de 6 meses dedicados a la adjudicación del contrato, ejecución de la obra civil e instalación de canaletas. Posterior a esto, se deberá realizar el tendido del cable, montaje de *racks*, armado y conexión de MDFs y SDFs, instalación de equipo activo y pruebas finales; para esto se estimó 4 meses adicionales aproximadamente.

4.1.2 RED HIPOTÉTICA DE DATOS PLANTEADA

La red que resultó de las acciones tomadas como una solución a corto plazo, se resume gráficamente en la figura 4.3.

Cada una de las estaciones conectadas a cada uno de los segmentos puede comunicarse con todos y cada uno de los servidores mostrados en la figura 4.3. La red funciona sobre los siguientes *stacks* de protocolos: IPX/SPX, TCP/IP, SNA.

Se debe considerar que cada uno de los segmentos de red (del 0 al 9) estará ubicado en su piso respectivo, es decir, el equipo de conectividad (*hubs*) del segmento 0 físicamente se encuentra instalado en la PB, el equipo de conectividad del segmento 1

está en el primer piso y así sucesivamente. El equipo de conectividad de los segmentos 10 y 11 físicamente están ubicados en el centro de cómputo, al igual que el equipo de conectividad del segmento 4. El centro de cómputo se encuentra ubicado en el cuarto piso.

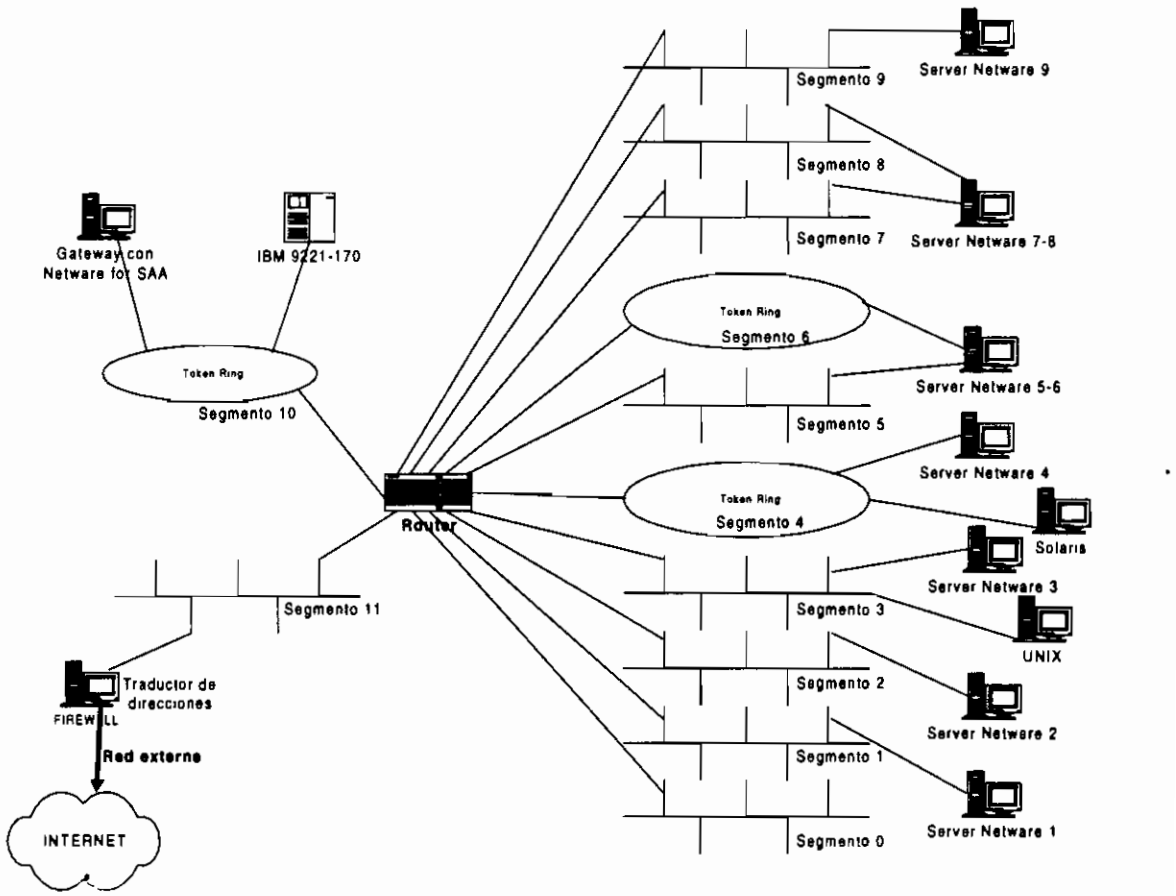


***Figura 4.3** Red hipotética de datos planteada como base para el análisis definitivo*

Todos los servidores mostrados en la figura 4.3 (Server Netware 1, 2, 3, ...,9, UNIX, Solaris, *Gateway* con *Netware for SAA* e IBM 9221), *firewall* y ruteador se encuentran físicamente ubicados en el centro de cómputo (cuarto piso), aunque las conexiones a los diferentes segmentos están realizadas como se muestra en la misma figura. La ventaja de tener estos equipos en el centro de cómputo, es facilitar la administración al mismo tiempo que se brinda mayor seguridad de los mismos.

4.1.3 ANÁLISIS DE LA RED HIPOTÉTICA PLANTEADA

La red hipotética de datos planteada será el foco de dos puntos de análisis:

- análisis cualitativo
- análisis cuantitativo

4.1.3.1 Análisis cualitativo

Se basa fundamentalmente en el conocimiento cualitativo de la utilización de los servicios de red en cada segmento y de la configuración de la red analizada.

El conocimiento cualitativo de la utilización de servicios de red, se lo puede obtener haciendo un breve estudio en el que se definan las principales fuentes de servicio de la red y los requerimientos de esos servicios por segmentos. No se requieren datos detallados.

El conocimiento cualitativo de la configuración de la red, se obtendrá en primer plano de un diagrama a grandes rasgos de la configuración de la red, y de los protocolos que tiene implementados. No se requieren datos detallados.

Pueden ayudar en este análisis algunos parámetros tales como:

- La cantidad aproximada de estaciones por segmento
- La distribución (concentrada o distribuida) de los equipos de conectividad
- Protocolos de comunicación implementados
- Ubicación de los puntos de fallo críticos

Una buena idea de estos datos los tiene generalmente el administrador de red o la persona que ha trabajado algún tiempo con la red, quien tiene noción de los sectores críticos de la red.

En función de esto, se puede generar un esquema cualitativo de flujo de tráfico que permitirá emitir determinados criterios iniciales.

El emitir criterios en función de un análisis cualitativo tiene las siguientes ventajas:

- Forman un diagnóstico inicial del estado de la red
- Este diagnóstico se genera en muy corto plazo
- El diagnóstico inicial en función de un análisis cualitativo, permite realizar un análisis cuantitativo con más criterio

Las principales debilidades de los criterios emitidos basándose en un análisis cualitativo son:

- Los datos cualitativos en función de los que se realiza el análisis podrían estar muy alejados de la realidad
- El emisor de criterios es recomendable que tenga experiencia de trabajo con redes, y mejor será si la tiene con la red analizada
- En algunas circunstancias los criterios cualitativos pueden sonar tan convincentes que podrían anular el requerimiento de un análisis cuantitativo

En general, es recomendable, que en cualquier análisis que se realice deba considerarse tanto la parte cualitativa como la cuantitativa; sin embargo, en determinadas circunstancias, en las que se requiera un criterio a priori y donde el riesgo en costo no sea significativo, bastará con un análisis cualitativo antes de implementar la solución.

Análisis cualitativo de la red propuesta

Del gráfico de la figura 4.3 se puede observar una LAN cuyos segmentos están en configuración colapsada hacia un ruteador "central". Debido a esta disposición, se debe notar que el ruteador es un punto crítico de falla.

Las estaciones de trabajo conectadas a cada uno de los segmentos de red, están en la posibilidad de utilizar los servicios provistos por los siguientes equipos:

a. *Mainframe* IBM 9221-170 a través del *gateway* con *Netware for SAA*
b. Servidores de red Netware
c. Servidores UNIX
d. Servidores Solaris
e. *Firewall* con traducción de direcciones

A. Conexión al *mainframe* IBM 9221-170

Cualquier estación de trabajo (en cualquier segmento de red) que tenga configurado el *stack* protocolos IPX/SPX y que posea un *software* de emulación adecuado, podrá conectarse al *mainframe* IBM a través del *gateway* que tiene instalado *Netware for SAA*. El *gateway* con *Netware for SAA* solo permitirán la conversión del protocolo IPX de Netware a SNA y viceversa. No realiza la conversión entre TCP/IP y SNA, para esto existen otros productos.

Los requerimientos de la conexión al *mainframe* IBM (por el tipo de trabajo que realizan los usuarios), vienen principalmente de los equipos conectados a los segmentos de red 0, 1, 7 y 8. Esto significa, que el tráfico generado por esta conexión fluirá principalmente entre estos segmentos y el segmento 10 (donde están conectados el *mainframe* y *gateway*) a través del ruteador.

Se debe notar que los paquetes transportados entre los segmentos de red y el *gateway* serán IPX, y solamente entre el *gateway* y el *mainframe* (en el segmento 10) se transportarán paquetes SNA.

B. Conexión a los servidores Netware

Cualquier estación (en cualquier segmento) que tenga instalado el *stack* de protocolos IPX/SPX podrá conectarse con cualquier servidor Netware (configurado con IPX/SPX por *default*) de cualquier segmento.

Las conexiones se disponen de tal forma que cada servidor Netware estuviera conectado directamente al segmento al cual da más servicio. Por ejemplo, el servidor Netware 2, está directamente conectado al segmento de red 2, pues es a este segmento al que más servicios presta. Con esta configuración se consigue minimizar el tráfico que cruzaría a través del ruteador, siempre y cuando todos los servidores estén configurados en un segmento dedicado[46]. Sin embargo, los requerimientos generados desde otros segmentos, necesariamente generarán tráfico en el ruteador hasta poder alcanzar el servidor requerido. Por ejemplo, si una estación del segmento 7 necesita un servicio del servidor 2, ese requerimiento tendrá que viajar a través del segmento 7, hasta llegar al ruteador, y salir por otro puerto del mismo ruteador hasta alcanzar el servidor 2 en el segmento correspondiente. Sin embargo este último tipo de requerimientos no es elevado, con excepción del servicio de correo electrónico que se presta.

Adicionalmente, debe notarse que en el segmento 0 no se tiene conectado servidor alguno, pero los usuarios de ese segmento normalmente utilizan los servicios que presta el servidor 1, generando de esta forma tráfico IPX entre los segmentos 0 y 1.

El tráfico generado por este motivo será netamente IPX/SPX.

C. Conexión a los servidores UNIX

Cualquier estación (en cualquier segmento) que tenga configurado el *stack* de protocolos TCP/IP, está en la posibilidad de utilizar los servicios brindados por los servidores UNIX.

Se debe notar que el servidor UNIX mostrado en la figura 4.3, está directamente conectado al segmento de red 3. Esto se debe a que son los usuarios de este segmento los que principalmente hacen uso del servicio que presta este servidor. Sin embargo, las aplicaciones que se han instalado sobre este servidor en el transcurso del tiempo, serán utilizadas por todos los usuarios de todos los segmentos (del 0 al 9) de la red.

Si se considera que esta última razón genera tráfico "ajeno" al segmento 3 en dicho segmento, sería conveniente pensar en cambiar la conexión de este servidor a un segmento dedicado. Otra razón para esta reconexión, es que los elementos de conectividad del segmento 3, pueden considerarse como puntos de fallo potenciales para un servicio que se presta a toda la entidad, siendo esto totalmente inconveniente.

D. Conexión a servidores Solaris

Cualquier estación (en cualquier segmento) que tenga configurado el *stack* de protocolos TCP/IP, está en la posibilidad de utilizar los servicios brindados por el servidor Solaris.

---

[46] La configuración en la que se forma un segmento dedicado para servidores es recomendable cuando se dispone de una buena infraestructura de transporte y un excelente subsistema de conectividad, capaz de soportar altas cargas de tráfico dirigidas a un solo segmento. Esta configuración se la propondrá posteriormente bajo otras condiciones.

El servidor Solaris se encuentra conectado directamente al segmento 4 de la red. Esto se debe a que son los usuarios conectados a este segmento los que más lo utilizan. Son también usuarios frecuentes aquellos cuyos equipos se conectan a los segmentos 5 y 6, es decir, por este motivo habrá tráfico que fluya entre los segmentos 5,6 y 4 a través del ruteador.

E. Conexión a Internet a través del traductor de direcciones

Cualquier estación que tenga configuración del *stack* TCP/IP, y pertenezca a uno de las subredes IP que están definidas en el traductor de direcciones podrá salir hacia Internet.

El traductor de direcciones IP se hace necesario, pues la red en estudio posee una red interna IP, es decir con direcciones que son para uso privado, mientras que para la utilización de servicios deben utilizarse direcciones convenidas y otorgadas por un organismo internacional. De esta forma, cualquier requerimiento que haga una estación con una dirección interna hacia el exterior, llegará hasta el traductor de direcciones, y éste lo hará parecer como un requerimiento generado por una estación con dirección externa.

4.1.3.2 Análisis cuantitativo

Se realiza en función de los siguientes parámetros:

- Tráfico por segmento (obtenido por mediciones realizadas con un analizador de protocolos) y determinado en función de estadísticas obtenidas en el transcurso del tiempo
- Capacidades de manejo de tráfico de los equipos de conectividad (obtenidas de los manuales del fabricante)
- Factores de utilización y crecimiento de red, tiempo de vida útil esperado y ancho de banda disponible

A. Tráfico por segmento

La medición de tráfico por segmento se realizó utilizando un producto de *software* denominado NetXray, el mismo que debe ser instalado en un computador que se conecte al segmento que desea ser analizado.

El resumen de los resultados obtenidos de las mediciones se muestra en la tabla 4.3; en la misma se observa el promedio de las mediciones que se realizaron durante 3 días por segmento.

Durante el período de mediciones, se realizaron varias pruebas de transmisión de tráfico de gráficos y videoconferencia (sin utilizar protocolos de compresión).

La transmisión de gráficos y sonidos, se la realizó instalando un CD de Windows 95 en una estación de trabajo y compartiendo su acceso hacia varias estaciones. Desde seis estaciones se realizaba la ejecución de un mismo archivo de movimiento y sonido (con extensión mov) a través de la red. El protocolo utilizado en la compartición era IPX/SPX. Adicionalmente, debe notarse que la red se encontraba trabajando con carga normal, precisamente para verificar el efecto que produce la transmisión de este tipo de tráfico. La prueba se realizó sobre los segmentos 4 y 11, obteniéndose los resultados mostrados en la tabla 4.4.

SEGMENTO	% TRAFICO IP	% TRAFICO IPX	Paquetes por segundo (promedio)	Paquetes por segundo (pico)	% UTILIZACION TOTAL PROMEDIO	% UTILIZACION TOTAL PICO
0	2.30	97.70	65.16	216.00	2.80	12.00
1	13.59	86.42	345.26	920.25	11.58	29.65
2	8.56	91.44	186.75	601.50	7.29	28.50
3	22.18	77.83	255.60	845.33	12.30	30.25
4	30.38	69.63	405.88	1004.00	13.13	31.63
5	20.63	79.38	431.88	872.50	18.13	33.75
6	11.88	88.13	228.75	594.88	15.00	33.25
7	10.25	89.75	262.30	896.65	15.10	30.65
8	14.66	85.35	396.57	1056.95	13.17	35.26
9	12.35	87.65	346.66	956.25	12.98	33.27
10	0.00	100.00	56.00	188.00	2.80	9.75
11	24.17	75.77	510.30	1346.30	14.60	54.70

Tabla 4.3 Resultados obtenidos del análisis de tráfico por segmento

SEGMENTO	% TRAFICO IP	% TRAFICO IPX	Paquetes por segundo (promedio)	Paquetes por segundo (pico)	% UTILIZACION TOTAL PROMEDIO	% UTILIZACION TOTAL PICO
4	11.50	88.50	1180.00	1615.00	38.80	68.00
11	8.50	91.50	1230.00	1850.00	46.80	79.00

Tabla 4.4 Resultados obtenidos de la medición de tráfico generado por archivos de video y audio en la red (a través de IPX)

SEGMENTO	% TRAFICO IP	% TRAFICO IPX	Paquetes por segundo (promedio)	Paquetes por segundo (pico)	% UTILIZACION TOTAL PROMEDIO	% UTILIZACION TOTAL PICO
4	82	18	1480	2710	85	96
11	85	22	1550	2810	85	98

Tabla 4.5 Resultados obtenidos de la medición de tráfico generado por videoconferencia unidireccional (sin compresión de datos) en la red (a través de IP)

La prueba de videoconferencia se la realizó empleando dos equipos SUN con SOLARIS 2.5 y utilizando una función propia del sistema para traer la imagen capturada en tiempo

real desde un equipo a otro. El equipo que capturaba la imagen estaba en el segmento 11, mientras que el que la recibía se encontraba en el segmento 4. Debe acotarse que el ancho de banda consumido para esta transmisión se marcaba en los equipos SUN como 5 Mbps. No se utilizó ningún tipo de compresión de datos para la transmisión de esta información. El protocolo utilizado era IP. Los resultados obtenidos se muestran en la tabla 4.5.

B. Capacidades de manejo de tráfico

Como puede observarse en la tabla 4.3, el porcentaje de utilización de tráfico en los segmentos de la red, se encuentran en rangos de funcionamiento normal. Debe notarse que la mayoría de analizadores de tráfico marcan como umbrales máximos al 40 ó 50 % para el porcentaje de utilización del segmento, y de 5000 paquetes por segundo para la velocidad de transmisión de paquetes por segmento. Se debe notar que en condiciones normales de trabajo ninguno de los segmentos se encuentra trabajando sobre esos umbrales.

La capacidad de manejo de tráfico del ruteador es de 25000 pps, suficiente para el manejo de tráfico de la red en estudio bajo condiciones normales. Sin embargo, si se empiezan a presentar condiciones como las planteadas en las pruebas, se notará que tanto los *hubs* de los segmentos como el ruteador (de *backbone*) comienzan a requerir mayor capacidad de manejo de tráfico.

C. Factores de crecimiento y utilización de la red

Se considera que una vez que se implemente una aplicación tipo multimedia para algunos usuarios de la red, su requerimiento entre el resto de usuarios empezará a ser alto. De esta forma, el porcentaje de utilización en los segmentos de red será tan alto, que será imposible manejar este tráfico utilizando dispositivos de conectividad de acceso compartido. Por ejemplo, si se estima que en uno de los segmentos, existen 6 usuarios (aproximadamente el 10% de usuarios del promedio de usuarios por segmento) que desean establecer una sesión de videoconferencia de alta calidad (se estima 1.5 Mbps de ancho de banda requerido por usuario cuando se utiliza compresión), se requeriría para este efecto un ancho de banda de 9 Mbps sólo para esta aplicación, lo que saturaría totalmente un segmento *Ethernet* 10BaseT y daría problemas a un segmento *Token-Ring* de 16 Mbps.

Considerando que todos los usuarios de la red deberían tener la posibilidad de manejar aplicaciones multimedia, se estima que cada usuario debería manejar al menos 1.5 Mbps dedicados a él, es decir utilizando un medio conmutado.

Si se considera que el promedio de usuarios por segmento es 60, se notará que en condiciones críticas, el conmutador del segmento debería estar en la posibilidad de manejar 90 Mbps (60 x 1.5 Mbps) en su *backplane*, y que el conmutador central (*backbone*) requeriría manejar aproximadamente 1 Gbps (11 x 90Mbps) en su *backplane* para la condición más crítica.

4.1.4 NUEVOS REQUERIMIENTOS DE RED

La entidad planteada tiene como objetivo, la implementación de un grupo de servidores de aplicaciones para toda la institución, y ya no la manutención de servidores departamentales que sirvan a un grupo de usuarios que pertenecen a determinado segmento como se ha visto hasta ahora. La ventaja principal de obtener esto, será el mejor aprovechamiento de los recursos disponibles en cuanto a *hardware*, *software*, administración de aplicaciones y sistemas operativos.

Entre otra de sus metas está la obtención de una red totalmente flexible a cualquier cambio o reubicación de equipo que fuera necesario. La flexibilidad en la infraestructura de transporte es cubierta con un buen diseño de la parte pasiva del cableado estructurado, lo cual se asume está bien realizado. Sin embargo, la flexibilidad del subsistema de conectividad debe lograrse con una buena implementación de protocolos de comunicación.

Finalmente, y entre los objetivos más exigentes, la entidad busca una red que soporte cualquier tipo de aplicaciones multimedia sobre ella. En nuestro medio, la existencia de redes con soporte de multimedia, es decir redes de multimedia, no es muy común. Normalmente la mayoría de aplicaciones de multimedia son soportadas a nivel de estación pero no a nivel de red.

La tecnología multimedia tiene un enfoque bastante definido, y apunta a sistemas distribuidos multimedia cuyos requerimientos fundamentales son:

- Transferencia de datos continua sobre períodos de tiempo relativamente altos
- Sincronización en el manejo de los diferentes tipos de datos (voz, sonido y video)
- Espacios de almacenamiento muy altos
- Manejo de tiempo real y técnicas especiales de indexamiento
- Recuperación de datos tipo multimedia

Las aplicaciones multimedia, especialmente la voz y el video, imponen requerimientos muy altos en cuanto a tiempo de despacho de datos dentro de una red. El tiempo de acceso, el ancho de banda y los retrasos en la transmisión están entre los parámetros más críticos de una red multimedia.

Para un mejor entendimiento del tipo de tráfico que puede manejarse, se hace su siguiente clasificación:

- *Tráfico no isocrónico*: Requiere una transparencia semántica y no una transparencia en tiempo, es decir, no tiene limitaciones estrictas de demora en su transferencia, pero la información debe llegar siempre a su destino. Este tipo de tráfico, generalmente viaja en ráfagas (un tiempo de actividad y otro de silencio). Ej: *transferencia de archivos y texto*

- *Tráfico isocrónico*: Requiere transparencia en tiempo y no en semántica, es decir, si se pierde poca información en el camino se puede recuperar el contexto. Ej: *transferencia de sonido, video.*

En un tipo de entidad como la analizada, se pueden emplear principalmente las siguientes aplicaciones de tipo multimedia que serían de gran utilidad como servicio a los usuarios de la red:

- *Correo multimedia:* Permite la edición multimedia del correo de voz, lo que requiere grandes tasas de transmisión comparadas con las utilizadas en el correo de texto.
- *Sistemas de trabajo colaborativo:* Donde los integrantes de un grupo de trabajo pueden discutir un problema desde sus estaciones de trabajo de manera simultánea. En esas reuniones pueden verse, discutirse y modificarse documentos multimedia.
- *Sistemas de conferencia:* Los grupos de usuarios que están en la capacidad de utilizar estos servicios pueden compartir reuniones remotamente, y desempeñar actividades donde se envíen y/o reciban video, audio y datos. Estas conferencias multimedia (video conferencias) manejan el concepto de "espacios de trabajo virtual compartido" el cual describe las partes del despliegue que son replicadas a todas las estaciones.

De lo señalado anteriormente, se debe resaltar que entre los principales requerimientos que hacen las aplicaciones multimedia a las redes están:

- Debe tenerse una demora máxima permitida en la entrega de unidades de información.
- Las pérdidas o unidades demoradas deben estar dentro de límites aceptables.
- La red debe estar en la capacidad de transmitir tráfico multimedia a múltiples destinos simultáneamente (punto a multipunto)

En la práctica, en la red hipotética planteada, se han realizado pruebas de multimedia sobre redes 10BaseT y *Token-Ring*, y se ha visto que puede funcionar siempre y cuando sean pocos los usuarios que accesan a ella. Sin embargo, estos tipos de tecnologías no están diseñados para transportar tráfico sincrónico como el audio y video, que requieren gran ancho de banda y tasa de transferencia constante.

4.2 CRITERIO DE DISEÑO Y NORMAS

En esta parte, se plantean los criterios que se tomarán en cuenta para el diseño de la red, haciendo énfasis en la parte del subsistema de conectividad, y de normas o protocolos de comunicación a utilizarse. Recúerdese que se asume la existencia de una infraestructura de transporte estructurada bien implementada. Sin embargo, serán los criterios que se den en esta parte, los que permitan definir la configuración a grandes rasgos que debe adoptar la mencionada infraestructura para satisfacer las necesidades del subsistema de conectividad.

4.2.1 CRITERIOS DE DISEÑO

Los criterios en función de los que se realizará el diseño de la red, son los siguientes:

- Experiencia
- Estandarización
- Funcionalidad actual
- Posibilitar un proceso de migración manteniendo recursos actuales
- Proyección futura en función de los requerimientos
- Tiempo de vida útil del proyecto
- Utilización de tecnología actual

4.2.1.1 Experiencia

Debe considerarse la evolución que ha tenido la red hipotética en estudio (numeral 4.1.1), y tomar en cuenta los aspectos negativos que se produjeron en el pasado, especialmente al permitir un crecimiento no planificado de la red.

4.2.1.2 Estandarización y homogeneidad

No solo el respetar los estándares recomendados por organizaciones mundiales garantizará un buen diseño de red, sino que deben mantenerse criterios de estandarización propios que permitan la obtención de una red organizada, en lo posible simétrica, uniforme, homogénea, con poca variedad de características, es decir evitando el tener una gama de productos para cada elemento de la red.

Por ejemplo, serán metas del diseño: poseer un mismo tipo de topología para cada segmento de red, eliminar en lo posible la variedad de estándares y protocolos en las capas 1, 2, 3 y 4 del modelo de referencia OSI.

Si bien el criterio de mantener una red homogénea en lo posible en todos los aspectos, requiere de una inversión inicial probablemente alta, los costos a largo plazo y en la fase de producción serán menores que los incurridos en una red sin esta característica.

4.2.1.3 Funcionalidad actual

Respetar la funcionalidad que tiene actualmente la red, en virtud del conocimiento que ha permitido obtener los análisis (cualitativo y cuantitativo) del numeral 4.1.3.

4.2.1.4 Posibilitar un proceso de migración manteniendo recursos actuales

El diseño como tal debe incluir un proceso de migración de la red actual hacia la red propuesta. Este criterio no sería necesario en el caso de contar con una red totalmente nueva.

Además, hay que considerar que parte de la tecnología actualmente utilizada en el subsistema de conectividad puede seguir funcionando con el nuevo diseño antes de llegar a su etapa final en el proceso migratorio. Tal podría ser el caso de las tarjetas de interfaz de red dependiendo del diseño que se vaya a seleccionar.

4.2.1.5 Proyección futura en función de los requerimientos

Uno de los aspectos que mayor importancia tiene en el diseño de la red, es el satisfacer las necesidades que se plantearon como requerimientos en el numeral 4.1.4.

Debe notarse que posiblemente no todos los usuarios utilizarán todas las aplicaciones planteadas en los requerimientos del numeral 4.1.4. Por esta razón, dentro del proceso de migración diseñado para la red, deben considerarse aspectos como éste y de esta forma dar prioridad de requerimientos a determinados sectores de la red. Esto podría estar en contrapunto con el criterio del literal b. (estandarización), de mantener en lo posible uniformidad en la red, sin embargo, en la práctica el pretender una red totalmente uniformizada u homogénea significa una inversión inicial bastante alta, a la cual no todas las entidades están en posibilidad de llegar.

4.2.1.6 Tiempo de vida útil del proyecto

Debe considerarse el tiempo de vida útil que se planea tenga el proyecto una vez implementado. Debido a que el tiempo de vida estimado para la parte pasiva del sistema de cableado estructurado, o como se lo ha definido en la presente tesis, la infraestructura de transporte, debe ser aproximadamente 15 años, debería considerarse un tiempo de vida útil similar para la parte activa o subsistema de conectividad. Sin embargo, esto se determina con mayor dificultad, pues la tecnología involucrada en el subsistema de conectividad se degrada más fácilmente y evoluciona con mayor velocidad que la infraestructura de transporte. Tomando en cuenta esta consideración, y recordando el gráfico de la figura 2.3 del capítulo II, donde se muestra el requerimiento en Kbps por usuario que se ha tenido y que probablemente se tenga en el futuro, se debería considerar que si el subsistema de conectividad debe tener un tiempo de vida útil de 10 años (hasta el año 2007)[47], y por tanto se estará hablando de un requerimiento por usuario de 10 Mbps.

[47] No se considera el grado de obsolescencia, sino la posibilidad económica que la entidad cambie de tecnología

4.2.1.7 Utilización de tecnología actual

En función de la proyección a futuro y del tiempo de vida estimado para el proyecto, es recomendable la utilización de la tecnología con mayor proyección a futuro, es decir que tenga características de escalabilidad, modularidad, compatibilidad hacia atrás, compatibilidad con otras tecnologías (sistemas abiertos), estabilidad, facilidad de administración, y en general que cumpla con especificaciones de estandarización mundiales.

La utilización de tecnología actual, permitirá que se cumpla con las características mencionadas en el párrafo anterior, pero adicionalmente es importante que la tecnología a utilizar haya sido probada y cuente ya con resultados satisfactorios de un amplio número de clientes. Desde este punto de vista es importante no caer en la tentación de utilizar tecnología "demasiado novedosa", porque posiblemente nos llevaría a ser tan solo un experimento de esa tecnología.

4.2.2 CRITERIOS PARA LA SELECCIÓN DE NORMAS O PROTOCOLOS DE COMUNICACIÓN

Las normas o protocolos de comunicación son parte fundamental en el buen desenvolvimiento de un subsistema de conectividad. Por esta razón es importante que se realice una evaluación de los protocolos a emplear en una red estructurada de datos.

4.2.2.1 Criterios Generales

Dentro de los criterios que deben considerarse para la elección de un *stack* de protocolos están:

- Difusión de los protocolos en el ámbito mundial
- Tendencia de los proveedores de aplicaciones
- Facilidad de administración
- Técnicas utilizadas por los protocolos

A. Difusión de los protocolos en el ámbito mundial

Debido principalmente a la integración de las redes en el ámbito mundial, debe pensarse en la selección de protocolos que permitan una fácil integración de las redes LAN con el resto de redes del mundo. La salida directa que está actualmente disponible como un medio de integración en el ámbito mundial es la red Internet.

B. Tendencia de los proveedores de aplicaciones

Esto posiblemente sea consecuencia del literal anterior, es decir, si se tiene mayor difusión en el ámbito mundial de un determinado producto, es lógico que los proveedores de aplicaciones utilicen este aspecto como coyuntura para vender sus productos.

A pesar de que los protocolos de comunicaciones deben estar abiertos a cualquier implementación de aplicaciones sobre ellos, en la práctica esto no es tan dable. Es decir, normalmente se han diseñado aplicaciones que funcionan sobre el grupo de protocolos de comunicaciones que pertenecen al mismo *stack*. Por ejemplo, aplicaciones como Telnet y FTP son diseñadas y forman parte del *stack* de protocolos TCP/IP.

En algunos casos, puede requerirse una aplicación que no pertenece al *stack* de protocolos disponible. Por ejemplo, supóngase la necesidad de realizar una transferencia de archivos desde un servidor Unix hasta un cliente Netware con IPX[48]. Esta operación puede ser atendida de varias maneras sin que el cliente IPX tenga que volverse un cliente IP, entre las cuales estaría: encapsulamiento del protocolo IPX dentro de IP, y adicionalmente la implementación de una aplicación NFS (*Network File System*). El encapsulamiento permitirá la comunicación entre el servidor Netware y el servidor UNIX, y la implementación de NFS, permitirá que el sistema de directorios de UNIX pueda ser visto desde un cliente Netware.

Este tipo de operaciones puede ser evitado si se cuenta con un *stack* al que los principales proveedores de aplicaciones consideran como primario para sus diseños. Desde esta perspectiva, se podría decir que la mayoría de proveedores han enfocado el desarrollo de sus aplicaciones para ser funcionales sobre TCP/IP en principio, y posteriormente sus productos son promocionados para el resto de *stack*s, con el consecuente desfase en tiempo de disponibilidad de esos productos para clientes que no utilizan TCP/IP.

C. Facilidad de administración

Esta característica afecta directamente al trabajo del administrador, pues será él la persona encargada de mantener la operatividad del protocolo.

Puede decirse que un protocolo de fácil administración será aquel que posee una característica de autoconfiguración, es decir la intervención del administrador para ponerlo operativo es muy poco representativa. Adicionalmente, un protocolo de fácil administración, permitirá que cualquier estación ubicada en cualquier segmento de red (obviamente del mismo tipo: *Ethernet*, *Token-Ring*), pueda ser cambiada sin ningún problema a otro segmento manteniendo su operatividad sin la necesidad de un cambio de configuración.

[48] Desde hace algún tiempo el sistema operativo Netware presenta soporte para redes TCP/IP

Adicionalmente, es importante que se considere un protocolo que facilite la administración del *hardware* sobre el que funciona, y sea compatible con protocolos de administración tales como SNMP.

D. Técnicas utilizadas por los protocolos

En los capítulos I y III de esta tesis ya se habló de cada una de las técnicas utilizadas por los protocolos en cada tema de cada nivel del modelo de referencia OSI.

Este criterio permite realizar una selección técnica de los protocolos que deben utilizarse dependiendo del requerimiento de comunicación que se tenga. En función de las técnicas que utilicen los diferentes protocolos, se puede tener un mejor entendimiento de su funcionamiento y de las fortalezas y falencias que posiblemente tengan.

4.2.2.2 Análisis de los protocolos utilizados en la red hipotética propuesta

Por el enfoque que se presenta en la tesis nos interesa el análisis de los protocolos de comunicación. Desde esta perspectiva, a continuación se presenta el análisis de la utilización de protocolos en las capas 3y 4, y posteriormente los utilizados en las capas 1 y 2.

El análisis se ha organizado de esta forma porque la funcionalidad que tienen los protocolos de las capas superiores (3 y 4) con los de las inferiores (1 y 2) es total. Es decir, cualquier implementación de las capas 3 y 4 funciona bien con casi cualquier implementación de las capas 1 y 2. Esto se explica porque el análisis podía haberse realizado de capa en capa, pero en la práctica hablar por ejemplo de un protocolo de la capa 3 es hablar de un *stack* de protocolos que involucra las capas 4, 5, 6 y 7, haciendo que el análisis de la capa 3 y 4 por separado sea innecesario.

Sin embargo, casi cualquier implementación de protocolos de las capas 3, 4 y superiores que pertenecen a un mismo *stack*, funciona bien sobre casi cualquier implementación de las capas 1 y 2.

A. Protocolos de capas 3 y 4

En la red hipotética propuesta, se manejan fundamentalmente tres *stack*s de protocolos de comunicación: IPX/SPX, TCP/IP, SNA. El *stack* SNA dentro de la red hipotética es cada vez menos importante en tráfico dentro de la red hipotética, debido principalmente a políticas adoptadas en cuanto a desarrollo de aplicaciones en ambientes cliente/servidor. Puede decirse que el tráfico más intenso dentro de la red es el generado por el *stack* IPX/SPX, debido principalmente a la gran distribución de servidores Netware en los segmentos de la red en estudio, seguido por el tráfico generado por el *stack* TCP/IP.

Debe destacarse, que la tendencia en el manejo de protocolos a nivel mundial, es el *stack* de protocolos TCP/IP, por las siguientes razones:

- Gran difusión en el ámbito mundial
- Rendimiento en enlaces con bajo ancho de banda
- Aplicaciones que soporta (principalmente de Internet)

Sin embargo, presenta sus desventajas principalmente en el campo de la administración, pues se requiere de un organismo internacional que mantenga organizada la red de direcciones en el ámbito mundial, y requiere además una delicada administración en el ámbito interno dentro de cada institución que maneja una red interna. Estos problemas han sido atendidos de alguna forma con implementaciones de asignaciones dinámicas de direcciones (DHCP), sin embargo, siguen siendo más difíciles de administrar que las redes IPX.

Otra gran desventaja del protocolo TCP/IP, cuando se dispone de una red IP que no es plana, es decir, donde se han definido subredes modificando las máscaras de *default*, es que si se desea modificar la ubicación de una estación de un segmento a otro con diferente dirección de red, la estación pierde su funcionalidad. Esto cuando no se tiene implementado la asignación dinámica de direcciones.

Todas las desventajas mencionadas anteriormente para TCP/IP, son transparentes para IPX/SPX. Sin embargo, la gran desventaja de IPX/SPX frente a TCP/IP, es su deficiente rendimiento en enlaces donde se dispone de bajo ancho de banda.

Una buena ventaja de TCP/IP es el desarrollo que soporta en cuanto a aplicaciones de administración de redes (SNMP) y su gran difusión a escala mundial.

La administración de una red es menos complicada, cuando se maneja la menor cantidad de protocolos posibles. Adicionalmente, la facilidad de administración que por si mismo representen los protocolos implementados, y fundamentalmente su proyección en el futuro en cuanto a aplicaciones que se desarrollen y funcionen con un buen desempeño sobre ellos, son aspectos que determinan la selección de un determinado protocolo.

Es importante señalar que debe considerarse el soporte de aplicaciones, mientras no se obtengan sistemas totalmente abiertos que adicionalmente proporcionen rendimiento similar sobre diferentes protocolos de capas más bajas que cumplan la misma función (IPX e IP por ejemplo). Es así, que varias aplicaciones desarrolladas a escala mundial, están orientando sus diseños para funcionar sobre ambientes TCP/IP, y opcionalmente sobre otros protocolos, pero obviamente estas implementaciones no llegan al mismo tiempo al otro tipo de cliente (DECnet, IPX/SPX, etc).

En conclusión, sería recomendable la utilización de un único *stack* de protocolos para ser implementado en una red, por facilidad de administración principalmente. Por su proyección, aplicaciones disponibles, rendimiento y difusión a escala mundial sería recomendable la utilización del *stack* de protocolos TCP/IP, en una estructura plana y utilizando asignación dinámica de direcciones.

Debe notarse que el párrafo anterior surge de una serie de razonamientos en cuanto a facilidad de administración, mejora de rendimiento y proyección hacia aplicaciones futuras, y no de la falta de disponibilidad de una adecuada infraestructura de transporte estructurada de datos. Es decir, sobre una infraestructura de transporte bien concebida, pueden combinarse varios *stacks* de protocolos con un buen rendimiento, pero con las consecuentes tareas adicionales para el administrador de la red y subsistema de conectividad.

B. Protocolos de capas 1 y 2

En la red hipotética planteada, los *stacks* de protocolos mencionados, funcionan sobre implementaciones 10BaseT y *Token-Ring*, es decir a 10 y 16 Mbps. Estos protocolos no están diseñados para transportar tráfico sincrónico como son el audio y video, principalmente *Ethernet* porque sus 10 Mbps no son suficientes para aplicaciones multimedia y las demoras que se presentan en la comunicación son no determinísticas. *Token-Ring* tiene la ventaja de ser un protocolo con demoras determinísticas por su método de acceso al medio (paso de testigo), sin embargo su velocidad de 16 Mbps sigue siendo baja para implementaciones en *backbone* y medios compartidos. Las implementaciones a 10 y 16 Mbps son compartidas en cada *hub* y utilizadas también en el *backbone*.

Debe recordarse que los requerimientos que imponen las aplicaciones multimedia están caracterizados por:

- Utilización de altos anchos de banda
- La mayoría de comunicaciones en redes multimedia son multipunto, a diferencia de las redes tradicionales que realizan comunicaciones punto a punto
- Las redes tradicionales son manejadas de tal manera que los datos estén libres de errores, sin embargo muchas aplicaciones multimedia pueden tolerar errores en su transmisión pero no demoras.

Considerando los puntos anteriores, debe tomarse en cuenta la utilización de protocolos que fueron clasificados en el capítulo III como protocolos de alta velocidad (FDDI, *Fast Ethernet*, ATM) y su desempeño con ambientes multimedia, para obtener una guía que permita recomendar el protocolo a utilizar dependiendo de la situación que se presente.

A continuación, se hará un breve resumen de algunas características de los protocolos de alta velocidad mencionados y su comportamiento en redes multimedia:

B.1 FDDI

Su velocidad de transmisión es 100 Mbps, suficientes para el manejo de información multimedia. Utiliza el método de acceso al medio conocido como paso de testigo, lo que hace que sea un protocolo determinístico, siendo ésta una característica que ayuda en la transmisión de información de tipo isocrónica. El protocolo MAC provee funciones para la iniciación del anillo y dos categorías de servicios: asincrónicas

y sincrónicas. Estas categorías definen la forma en que se captura el testigo. Cualquier estación puede emplear cualquiera de las dos prioridades.

En el servicio sincrónico cada estación tiene asignado un ancho de banda sincrónico (SBA *Synchronous Bandwitdth Allocation*) usando un protocolo de manejo. A la estación se le permite capturar el *token* y originar mensajes cada vez que éste pasa por ella. Este método da un tiempo de latencia bajo comparado con el otro tipo de servicio.

El servicio asincrónico divide el ancho de banda no consumido por el *synchronous allocation* entre todas las estaciones. Para realizar esto, cada estación mantiene un temporizador (TRT *Token Rotation Timer*) que es puesto en cero cada vez que el *token* pasa por la estación. Cuando la siguiente estación recibe el *token*, compara el TRT con otro temporizador de referencia (TTRT Target *Token* rotation timer), generalmente configurado en 8 ms. Si TRT<TTRT el momento en que el *token* pasa por la estación, el *token* es atrapado por ella, sin embargo, si TRT>TTRT se dice que el *token* está retrasado y las estaciones que están limitadas a prioridad asincrónica deben ceder el *token* a las estaciones sincrónicas.

De esta forma, si la carga es suficiente para saturar el anillo, pero la mayor parte del tráfico es asincrónico, el retraso máximo de acceso para cada una de las N estaciones puede calcularse así:

- Retraso sincrónico: 2 * TTRT (nominalmente 16ms)
- Retraso asincrónico: N * TTRT

FDDI presenta bajos tiempos de retardo en modo sincrónico (por su característica de prioridad sincrónica) tanto en la transmisión como entre la llegada de los distintos paquetes de información, sin embargo, su diseño está orientado hacia *backbone*s y por precio no a estaciones de trabajo.

FDDI es una tecnología madura que está completamente estandarizada, lo que garantiza facilidad en la adquisición de equipos y su compatibilidad entre distintos fabricantes.

Teóricamente, en una red FDDI (100 Mbps) pueden enviarse simultáneamente 66 videos (MPEG) de 1.5 Mbps cada uno, sin embargo un diseño tan ajustado podría generar problemas. La transmisión de un archivo (tráfico en ráfaga) puede acaparar momentáneamente el medio y dañar el envío de todos los videos. Por esta razón, es recomendable que cuando se utilice FDDI se haga un diseño bastante holgado para la transmisión de archivos, previniendo el envío de ráfagas.

B.2 *Fast Ethernet*

Puede decirse que *Fast Ethernet* es la implementación 802.3 pero a 100Mbps. Las estaciones se conectan a la red sin necesidad de que el MAC realice iniciación alguna, lo que simplifica su implementación.

Al igual que 10BaseT, *Fast Ethernet* o 100BaseT, utilizan el método de acceso CSMA/CD, es decir, antes de iniciar la transmisión, una estación escucha el canal para asegurarse que no está ocupado. Luego la estación transmite, mientras se monitorea una señal de colisión para asegurarse que la transmisión no ha experimentado una colisión. Si no se detecta una colisión, la estación invoca un algoritmo, que vuelve a programar la estación para que sea realizada en un tiempo seleccionado aleatoriamente en el futuro.

Por su diseño, *Fast Ethernet* es un protocolo no determinístico, que no proporciona control de latencia, al igual que 10BaseT, lo que hace que no pueda garantizar isocronismo en el despacho y llegada de paquetes. Sin embargo, debido a que maneja una tasa de bits de 100 Mbps, en redes en las que no hay mucho tráfico isocrónico, la probabilidad de que los paquetes lleguen a tiempo es muy alta.

Fast Ethernet tiene la ventaja de ser fácilmente migrable desde redes 10BaseT.

B.3 ATM

ATM es un protocolo orientado a conexión, punto a punto y punto a multipunto, full dúplex, el cual utiliza un pequeño paquete de tamaño fijo llamado celda. Debido a que éste es un formato para ser usado por conmutadores, no es necesario un protocolo de arbitraje para el acceso al medio.

Por su diseño, presenta un gran desempeño ante señales isocrónicas, ya que el protocolo UNI de ATM clasifica los servicios en varias clases, lo que emplea para reservar el ancho de banda en el momento de establecer el circuito virtual conmutado, asegurando de esta forma una buena calidad de servicio para todos los circuitos que logren establecerse.

La madurez de este protocolo podría decirse que está avanzando, sin embargo, parece que existen todavía algunas disputas entre los proveedores. Por este motivo, si se opta por esta tecnología sería preferible hacerlo con productos de un mismo fabricante para garantizar conectividad.

ATM funcionando al servicio de redes multimedia, tiene la ventaja de haber sido diseñado para todo tipo de tráfico, lo que permite que se garantice el servicio. Otros protocolos de altas velocidades, pueden manejar tráfico multimedia por su gran velocidad, siempre y cuando se mantenga una red holgada de este tipo de tráfico.

B.4 Gigabit Ethernet

Es un protocolo relativamente nuevo, que se basa en las especificaciones 802.3, incluyendo su método de acceso a medios CSMA/CD. Sin embargo su velocidad de transmisión alcanza los 1000 Mbps. Es decir, es un protocolo semejante a *Fast Ethernet* en concepto, pero 10 veces más rápido.

Fundamentalmente tiene dos ventajas:

- Sus promotores garantizan total compatibilidad con estándares del grupo 802.3 y *Fast Ethernet.*
- Su alta velocidad posiblemente permita el manejo de tráfico isocrónico de una manera satisfactoria, pese a ser un protocolo no diseñado para ese objetivo. Lo que si se puede garantizar es un excelente desempeño en redes que manejan altas cargas de tráfico no isocrónico.

Su principal desventaja, precisamente es el no estar diseñado para manejo de tráfico multimedia.

A pesar de no ser un estándar oficial (802.3z), el Instituto de Ingenieros Eléctricos y Electrónicos (IEEE), terminó su revisión sobre este protocolo en Marzo de este año, y se espera que no se presenten modificaciones ni funciones añadidas a esta tecnología en el futuro. Actualmente, se está tratando de compilar todas las especificaciones para *Gigabit Ethernet* y se espera tenerlas listas para principios de 1998.

4.3 ALTERNATIVAS DE UN SUBSISTEMA DE CONECTIVIDAD DE UNA RED DE DATOS PARA SU INTEGRACIÓN SOBRE UN SISTEMA DE CABLEADO ESTRUCTURADO Y PARÁMETROS QUE GUIAN A LA MEJOR SELECCIÓN TÉCNICA

Hasta el momento se ha realizado el análisis de la red actual, se han planteado nuevos requerimientos y varios criterios que serán la guía para la determinación del diseño y utilización de protocolos de comunicación.

4.3.1 DISEÑO DE RED TOPOLÓGICA GLOBAL

A partir de la red hipotética actual mostrada en la figura 4.3, y de los nuevos requerimientos que tendrá que afrontar esta red en el futuro, se sugiere el diseño de topología global presentado en la figura 4.4.

Este diseño inicial de diseño global se genera principalmente en la necesidad de establecer un FARM de servidores, debido al cambio de concepción que se presentó anteriormente, en el que se mencionaba que la nueva red requería implementar servidores ya no departamentales, sino servidores de aplicaciones institucionales.

Si se compara las figuras 4.3 y 4.4, se notará que el cambio de topología global prácticamente no ha cambiado, con excepción de la conexión del FARM de servidores, que ahora se encuentra conectada hacia un único concentrador, mientras que anteriormente estos servidores se ubicaban distribuidos en cada segmento.

Se puede notar además, que mientras anteriormente se disponían de varios posibles puntos de falla distribuidos en cada segmento con la conexión a los servidores,

al momento se tiene un único punto de falla pero más crítico. Es más crítico porque en caso de fallar, el efecto se reflejaría a todos los usuarios de la red, mientras que anteriormente, si fallaba el servidor conectado al segmento 9, por su concepción de servicio departamental, serían principalmente sólo los usuarios de ese segmento los afectados. Con la concepción de servidores de aplicaciones institucionales, el riesgo es mayor, pero se optimizan recursos en los servidores. Para contrarrestar el riesgo de falla, deben implementarse sistemas redundantes tolerantes a fallas.

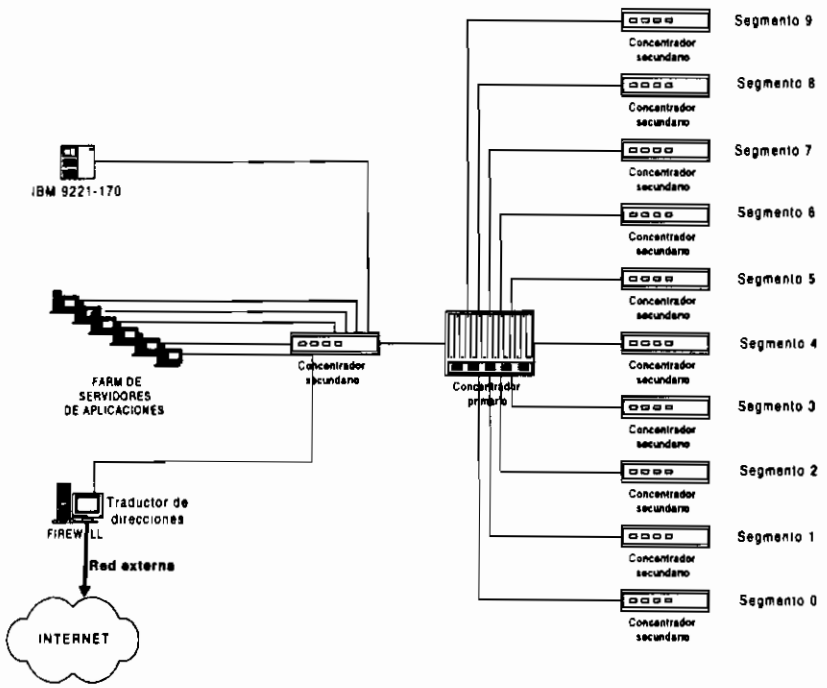


***Figura 4.4** Diseño de topología global*

Los usuarios en cada segmento (del 0 al 9) se conectarán a través del cableado de tendido horizontal de la infraestructura de transporte hasta un *patch panel* de piso, y a través de éste al elemento de conectividad que hemos definido como concentrador secundario en cada segmento. Se puede observar que en la figura 4.4, solo se diagrama el subsistema de conectividad, pues es claro que el sistema será implementado sobre una infraestructura de transporte que fue previamente diseñada.

De la figura 4.4, es fácil concluir que el flujo de tráfico estará pasando a través del concentrador principal, entre el concentrador secundario de servidores y los concentradores secundarios de pisos (segmentos del 0 al 9).

Debe señalarse que hasta el momento no se ha definido el tipo de equipo de conectividad para ninguno de los concentradores secundarios ni principal. Es decir, no se ha decidido si el concentrador principal deba ser un ruteador, conmutador o simplemente un *hub*, ni se ha decidido qué tipo de equipos son los concentradores secundarios. La determinación de estos elementos deberá realizarse en función de los nuevos requerimientos planteados en el numeral 4.1.4 y guiados por los criterios planteados en el numeral 4.2 de este capítulo.

De las recomendaciones de diseño realizadas por el estudio de cableado estructurado, se ve que en la parte de infraestructura de transporte no se tienen limitaciones en cuanto a ancho de banda, pues la tabla 4.2 muestra que en el *backbone* se utiliza fibra óptica desde el concentrador principal hasta cada uno de los secundarios. y en el cableado horizontal se utilizan cables UTP categoría 5. De esto, se puede prever que la conectorización, es decir los cables entre los concentradores secundarios y el principal utilizarán conectores para fibra, y los conectores de los concentradores secundarios que se conecten al cableado horizontal de usuarios, utilizarán polarización WE8E o más conocida como RJ45.

4.3.2 POSIBLES COMBINACIONES DE DISPOSITIVOS Y TECNOLOGÍAS DEL SUBSISTEMA DE CONECTIVIDAD

Las posibles combinaciones de dispositivos y tecnologías para el subsistema de conectividad planteado de manera global en la figura 4.4 y siguiendo los criterios del numeral 4.2 se muestran en la tabla 4.6.

En la tabla 4.6, pueden notarse 3 tipos de dispositivos de conectividad elegibles:

- *Ruteador*: Dispositivo que actúa hasta la capa 3, pero que tiene velocidad de procesamiento de paquetes limitada debido a los procesos que realiza en tiempo real. El ancho de banda que posee lo comparten los dispositivos que se conectan con él.
- *Switch*: Dispositivo que actúa hasta la capa 2, pero posee altas velocidades de procesamiento de paquetes y garantiza un ancho de banda dedicado a cada puerto.
- *Hub*: Dispositivo que actúa en la capa física (capa 1), sirviendo simplemente como centro de concentración, y compartiendo su ancho de banda entre todos los que se conectan a él.

Además, en la tabla 4.6 se han clasificado dos tipos de tecnologías disponibles:

- *Tradicionales*: Aquellas de relativa baja velocidad, por ejemplo: *Ethernet* 10BaseT, *Token-Ring*.
- *Alta velocidad*: Aquellas que funcionan a altas velocidades, por ejemplo: FDDI, *Fast Ethernet*, ATM, *Gigabit Ethernet*.

La tabla 4.6 debe entenderse de la siguiente forma:

- Es factible la combinación de dispositivos de conectividad y tecnologías en el orden presentado en la tabla y no en otras combinaciones (también posibles matemáticamente), pues la tabla está ordenada jerárquicamente de más a menos. Es decir, no sería técnicamente recomendable proponer la combinación: *Hub* para el concentrador principal, y *switches* para los secundarios, pues dada la configuración planteada en el diseño topológico de la figura 4.4, el *hub* se convertiría en un "cuello de botella" para los

switches, desperdiciando totalmente la inversión en los *switches*. Situación análoga ocurre con la combinación de tecnologías.

- La nomenclatura o código de diseño X.n (ej: A.1, B.1, C.3, E.4) debe entenderse de la siguiente forma:

X= Combinación de dispositivos de conectividad (X puede ser igual a A, B, C, D, E o F) donde:
A= *SWITCH-HUB-HUB* (**S-H-H**)
B= *SWITCH-SWITCH-HUB* (**S-S-H**)
C= *SWITCH-SWITCH-SWITCH* (**S-S-S**)
D= ROUTER-*HUB-HUB* (**R-H-H**)
E= ROUTER-*SWITCH-HUB* (**R-S-H**)
F= ROUTER-*SWITCH-SWITCH* (**R-S-S**)
n= Combinación de tecnologías (n puede ser igual a 1, 2, 3 ó 4) donde:
1= Tradicional-Tradicional-Tradicional (**T-T-T**)
2= Alta veloc.-Tradicional-Tradicional (**A-T-T**)
3= Alta veloc.- Alta veloc.-Tradicional (**A-A-T**)
4= Alta veloc.- Alta veloc.- Alta veloc. (**A-A-A**)

Diseño	Tipo de dispositivo de conectividad (concentrador principal)	Tipo de dispositivo de conectividad (concentrador secundario de servidores)	Tipo de dispositivo de conectividad (concentradores secundarios de segmentos 0-9)	Tecnología de *backbone* (entre concentrador principal y secundarios)	Tecnología hacia los servidores (entre concentrador de servidores y servidores)	Tecnología hacia las estaciones de usuarios (entre concentradores secundarios y equipos de usuarios)
A.1	*SWITCH*	*HUB*	*HUB*	Tradicional	Tradicional	Tradicional
A.2	*SWITCH*	*HUB*	*HUB*	Alta veloc.	Tradicional	Tradicional
A.3	*SWITCH*	*HUB*	*HUB*	Alta veloc.	Alta veloc.	Tradicional
A.4	*SWITCH*	*HUB*	*HUB*	Alta veloc.	Alta veloc.	Alta veloc.
B.1	*SWITCH*	*SWITCH*	*HUB*	Tradicional	Tradicional	Tradicional
B.2	*SWITCH*	*SWITCH*	*HUB*	Alta veloc.	Tradicional	Tradicional
B.3	*SWITCH*	*SWITCH*	*HUB*	Alta veloc.	Alta veloc.	Tradicional
B.4	*SWITCH*	*SWITCH*	*HUB*	Alta veloc.	Alta veloc.	Alta veloc.
C.1	*SWITCH*	*SWITCH*	*SWITCH*	Tradicional	Tradicional	Tradicional
C.2	*SWITCH*	*SWITCH*	*SWITCH*	Alta veloc.	Tradicional	Tradicional
C.3	*SWITCH*	*SWITCH*	*SWITCH*	Alta veloc.	Alta veloc.	Tradicional
C.4	*SWITCH*	*SWITCH*	*SWITCH*	Alta veloc.	Alta veloc.	Alta veloc.
D.1	RUTEADOR	*HUB*	*HUB*	Tradicional	Tradicional	Tradicional
D.2	RUTEADOR	*HUB*	*HUB*	Alta veloc.	Tradicional	Tradicional
D.3	RUTEADOR	*HUB*	*HUB*	Alta veloc.	Alta veloc.	Tradicional
D.4	RUTEADOR	*HUB*	*HUB*	Alta veloc.	Alta veloc.	Alta veloc.
E.1	RUTEADOR	*SWITCH*	*HUB*	Tradicional	Tradicional	Tradicional
E.2	RUTEADOR	*SWITCH*	*HUB*	Alta veloc.	Tradicional	Tradicional
E.3	RUTEADOR	*SWITCH*	*HUB*	Alta veloc.	Alta veloc.	Tradicional
E.4	RUTEADOR	*SWITCH*	*HUB*	Alta veloc.	Alta veloc.	Alta veloc.
F.1	RUTEADOR	*SWITCH*	*SWITCH*	Tradicional	Tradicional	Tradicional
F.2	RUTEADOR	*SWITCH*	*SWITCH*	Alta veloc.	Tradicional	Tradicional
F.3	RUTEADOR	*SWITCH*	*SWITCH*	Alta veloc.	Alta veloc.	Tradicional
F.4	RUTEADOR	*SWITCH*	*SWITCH*	Alta veloc.	Alta veloc.	Alta veloc.

***Tabla 4.6** Posibles configuraciones de diseño de conectividad para el diseño de topología global de la figura 4.4*

Código de diseño (X.n) con n fijo	Fortalezas	Debilidades
A.n *(S-H-H)*	• Combinación de dispositivos relativamente económica • Buen manejo de cargas de tráfico en *backbone*	• Posible "cuello de botella" en *HUB* de servidores durante cargas altas de tráfico • No recomendable para altas cargas de tráfico desde estaciones • No se realiza ruteo de protocolos de capa 3
B.n *(S-S-H)*	• Combinación de dispositivos menos económica que la combinación de dispositivos **A.n** • Buen manejo de cargas de tráfico en *backbone* y servidores	• No recomendable para altas cargas de tráfico desde estaciones • No se realiza ruteo de protocolos de capa 3
C.n *(S-S-S)*	• Combinación de dispositivos de alto costo global • Buen manejo de cargas de tráfico en toda la red	• No se realiza ruteo de protocolos de capa 3
D.n *(R-H-H)*	• Combinación de dispositivos relativamente económica • Suficiente para cargas de trabajo medias y bajas • Se tiene ruteo de protocolos de capa 3	• Ruteador posible "cuello de botella" en la red • Posible "cuello de botella" en *HUB* de servidores bajo cargas altas de requerimientos • No recomendable en altas cargas de tráfico
E.n *(R-S-H)*	• Combinación de dispositivos menos económica que **D.n** • Suficiente para cargas de trabajo medias y bajas • Servidores responden mejor bajo altas cargas de requerimientos • Se tiene ruteo de protocolos de capa 3	• Posible "cuello de botella" en el ruteador central • No recomendable en altas cargas de tráfico
F.n *(R-S-S)*	• Combinación de dispositivos de alto costo global • Buen desempeño de la red para cargas de trabajo medianamente altas • Se tiene ruteo de protocolos de capa 3	• Posible "cuello de botella" en el ruteador central • No recomendable en altas cargas de tráfico

Tabla 4.7 Fortalezas y debilidades de las posibles combinaciones de dispositivos de conectividad propuestas en la tabla 4.6

Para un mejor entendimiento, propongamos el diseño B.2 (ver tabla 4.6) como ejemplo, y veamos como debería entenderse ese diseño:

- El diseño dice que la red está formada por un *switch* central (concentrador principal), un *switch* para conexión con los servidores (concentrador secundario de servidores) y *hubs* para la conexión con las estaciones de los diferentes segmentos (concentradores secundarios de los segmentos del 0 al 9).
- De la tecnología utilizada en el *backbone* se desprende que se utilizará una tecnología de alta velocidad para la conexión del *switch* de servidores al *switch* principal, y de los *hubs* al *switch* principal. Las conexiones desde el *switch* principal tendrán garantizados un ancho de banda dedicado tanto a los *hubs* como al *switch* de servidores.

- De la tecnología utilizada hacia los servidores, debe entenderse que del *switch* de servidores hacia los servidores está utilizando tecnología tradicional, pero, por el hecho de ser *switch*, se garantiza un ancho de banda dedicado a cada uno de los servidores conectados a él.
- De la tecnología utilizada hacia las estaciones, debe entenderse que de cada uno de los *hubs* de segmento (del 0 al 9), las conexiones a las estaciones utilizan tecnología tradicional. Por el hecho de ser *hubs*, todas las estaciones conectadas a cada *hub* compartirán un ancho de banda.

En la tabla 4.7, se muestran algunas fortalezas y debilidades para cada posible combinación de dispositivos de conectividad que se mostró en la tabla 4.6, pero sin considerar la influencia de la combinación de tecnologías para estos dispositivos (con n fijo).

En la tabla 4.8, se muestran algunas fortalezas y debilidades para cada posible combinación de tecnologías en los dispositivos de conectividad que se mostró en la tabla 4.6, pero sin considerar la influencia de la combinación de dispositivos de conectividad (con X fijo).

La combinación de las tablas 4.7 y 4.8, los nuevos requerimientos planteados y los criterios propuestos como guías para el diseño de red, servirán para determinar el tipo de dispositivos y tecnologías a utilizar sobre el diseño de topología global mostrado en la figura 4.4.

Código de diseño (X.n) con X fijo	**Fortalezas**	**Debilidades**
X.1 *(T-T-T)*	• Bajo costo relativo • Combinación de tecnologías suficiente para redes de tráfico no isocrónico	• No recomendable para tráfico isocrónico
X.2 *(A-T-T)*	• Bajo costo relativo • Combinación de tecnologías proporciona buen rendimiento para red de tráfico no isocrónico • Tolera tráfico isocrónico en bajas proporciones	• No recomendable para tráfico isocrónico con cargas medias o altas
X.3 *(A-A-T)*	• Costo relativo bajo, pero menos bajo que en X.2 • Combinación de tecnologías suficiente para cargas medias de tráfico isocrónico	• No recomendable para tráfico isocrónico con cargas altas
X.4 *(A-A-A)*	• Combinación de tecnologías proporciona buen rendimiento ante tráfico isocrónico	• Costo relativo alto porque cambio de tecnología también involucra a estaciones de trabajo

Tabla 4.8 Fortalezas y debilidades de las posibles combinaciones de tecnologías propuestas en la tabla 4.6

De los nuevos requerimientos planteados, se concluye que se necesita una red que soporte a corto plazo medianas capacidades de tráfico isocrónico y altas de tráfico no isocrónico. Entre uno de las metas del proyecto, se supone un diseño que contemple

una red que dure muchos años y que sea escalable tecnológicamente en el tiempo. De esto se deriva, que como alcance a largo plazo (algunos años) la red deberá estar en capacidad de transmitir grandes cantidades de tráfico de cualquier tipo.

Al hablar de la necesidad de manejar grandes cantidades de tráfico de cualquier tipo, se debería escoger un diseño que soporte esta característica en cuanto a combinación de dispositivos y tecnologías. De esto se concluye que (ver tablas 4.7 y 4.8):

- Entre las combinaciones de dispositivos que convienen están: B.n ***(S-S-H)*** y C.n ***(S-S-S)***
- Entre las combinaciones de tecnologías que convienen están: X.3 ***(A-A-T)*** y X.4 ***(A-A-A)***

De esta selección se podría tener cuatro opciones (ver tabla 4.6): B.3, B.4, C.3, C.4. Estas opciones tienen las ventajas y desventajas mostradas en la tabla 4.9.

Diseño	Ventajas	Desventajas
B.3	a. Para su implementación se evitaría la compra de tarjetas que existen sobre el ambiente LAN tradicional de cada segmento, con excepción de los segmentos *Token-Ring* si se desea migrar hacia *Ethernet*. b. Si quisieran aprovecharse los *hubs* que se utilizan en la red actual, para disminuir costos frente a una necesidad actual no tan exigente, se podría solicitar un módulo con varios puertos de LAN tradicional para ser instalado en el *switch* central y desde ahí conectar los *hubs* de piso.	a. Las estaciones se conectan a los *Hubs* de tecnología tradicional en un ambiente compartido y no conmutado. b. La tecnología tradicional compartida en estaciones rompería todo el esquema de manejo de altas tasas de tráfico isocrónico y no isocrónico. c. Si se optase por la compra del módulo sugerido en el literal b. de las ventajas, este módulo dejaría de ser útil el momento de una implementación con tecnología de alta velocidad.
B.4	a. Dependiendo de la tecnología de alta velocidad que se utilice en los *hubs* de piso, podría no ser necesaria la compra inmediata de interfaces de red para las estaciones (ej: si se opta por 10/100 BaseT *autosensing*)	a. Las estaciones se conectan a los *Hubs* de protocolos con tecnología de alta velocidad, pero en un ambiente compartido y no conmutado. b. Mientras no se cambien las interfaces de red tradicionales de las estaciones a interfaces de alta velocidad, no podrán manejarse altas tasas de tráfico, y menos de tráfico isocrónico.
C.3	a. Pueden utilizarse las interfaces de red que poseen actualmente las estaciones b. La fase de implementación se reduciría al área de *backbone* y servidores	a. Las estaciones se conectan a los *Hubs* de tecnología tradicional pero en un ambiente conmutado. b. Esta implementación podría ser insuficiente para necesidades de mediano-largo plazo (algunos años), cuando las aplicaciones exijan grandes tasas de tráfico de cualquier tipo.
C.4	a. La implementación de este diseño es la que más tiempo de vida útil tendrá b. Presenta funcionalidad para cualquier tipo de aplicación que exija altas tasas de cualquier tipo de tráfico.	a. Esta implementación exigiría una inversión inicial muy alta debido a las condiciones actuales de la tecnología de estaciones principalmente. b. Si la compra de los *switches* de segmentos es demasiado temprana para las reales necesidades del presente y del futuro a mediano plazo (2 ó 3 años), sería conveniente esperar hasta que realmente las necesidades lo exijan y en ese tiempo se comprarían equipos seguramente con mejores características.

Tabla 4.9 Ventajas y desventajas de las alternativas seleccionadas como posibles soluciones de subsistema de conectividad

Debe observarse que en las cuatro configuraciones elegidas, el concentrador central de *backbone* es un *switch*. Debido a que el *switch* es un dispositivo de conectividad que actúa en la capa 2, no realiza funciones de enrutamiento de protocolos de capa 3 como IP e IPX. Si se quisieran conservar estas funciones de enrutamiento, debería pensarse en un ruteador central o un ruteador anexo al *switch* central. Sin embargo, esta última opción generaría demoras en la transmisión de información producto de las operaciones de enrutamiento.

Para evitar la presencia de un ruteador y mantener el funcionamiento de protocolos de capas superiores (IP, IPX), debe procederse a un aplanamiento de esos protocolos, es decir eliminar las subredes existentes.

La eliminación de subredes en el protocolo IPX es muy sencilla, pues esta configuración se guarda tan solo en los puntos de unión de segmentos, por ejemplo: ruteadores, servidores.

La eliminación de subredes en el protocolo IP es más laboriosa, debido a que esta configuración se guarda incluso en las estaciones de trabajo. El aplanamiento se obtiene fijando las direcciones IP con su máscara de *default*, y definiendo como *gateway* a su propia dirección y no la de un puerto de ruteador. La ventaja de esto es que cualquier estación podrá reubicarse en cualquier sitio de la red sin requerir reconfiguración en su dirección IP. Sin embargo, la desventaja será que se tendrá un único dominio de tráfico, en el que están incluidos *broadcast* y *multicast*.

Se debe recordar que la segmentación de redes se utiliza para definir dominios de tráfico, evitando de esa manera que toda la red se inunde con tráfico innecesario. Si se eliminan estas subredes, se tendrá un solo dominio de tráfico, lo que hará que la red se inunde de tráfico de *broadcast* y *multicast* innecesario.

Realmente, en cualquiera de las posibles soluciones es necesario tener un solo dominio IP o IPX de tráfico ya que los conmutadores (*switches*) no pueden manejar subredes como los ruteadores. Eso significa, que se tendrá un único dominio de tráfico IP, y un único dominio de tráfico IPX con las desventajas ya mencionadas. Sin embargo, los conmutadores introducen un concepto muy interesante conocido como redes virtuales.

En el capítulo III se habló sobre las redes virtuales, y se dijo que son la forma en la que los conmutadores manejan dominios de tráfico. También se dijo que existen conmutadores que realizan funciones de enrutamiento entre redes virtuales (que no es lo mismo que enrutar protocolos de capa 3).

Si bien se tendrá un único dominio IP y un único dominio IPX, el tráfico puede ser controlado por la definición de redes virtuales en la red.

4.3.3 SELECCIÓN DEL DISEÑO DEFINITIVO

Hasta el momento, la selección de alternativas "finalistas" ha servido como un marco de lineamientos generales que conducen hacia un diseño más fino que determine con más detalle los dispositivos y tecnologías a utilizar en el diseño definitivo.

Entre las sugerencias que se mencionaron dentro del estudio de cableado estructurado, estuvo la de mantener redes tipo *Ethernet* para las estaciones de trabajo, conectadas a un *backbone* de fibra con tecnologías de alta velocidad (mínimo 100 Mbps).

Luego del desarrollo que hasta el momento se ha seguido, los resultados son semejantes a los sugeridos en el estudio. Es claro que de la tabla 4.7 se determina la utilización de conmutadores con tecnologías de alta velocidad (protocolos de alta velocidad) tanto para el concentrador principal como para el concentrador de servidores presentados en la figura 4.4. La diferencia hasta el momento, está principalmente en la determinación del tipo de dispositivos y tecnologías a utilizarse en los segmentos que sirven a los usuarios.

Considerando que la necesidad de manejar tráfico isocrónico al momento será requerida a corto plazo por la minoría de estaciones de trabajo y considerando que el porcentaje de utilización en la red tiene todavía posibilidad de crecer de acuerdo al análisis cuantitativo presentado en el numeral 4.1.3.2, puede plantearse la siguiente alternativa referente a los dispositivos de segmentos de usuario:

- Mantener las interfaces de estaciones de trabajo de tecnologías *Ethernet* 10BaseT instaladas (mayoría), y migrar las tecnologías *Token-Ring* existentes (minoría) a *Ethernet*, con el objeto de estandarizar tecnologías (esto facilita la administración de estaciones de trabajo).
- Los dispositivos de conectividad para los concentradores secundarios de usuarios, serán conmutadores totalmente modulares con facilidades de escalabilidad por módulos. De esta forma puede adquirirse inicialmente módulos con puertos conmutados 10BaseT, y posteriormente según las necesidades lo requieran ir agregando o migrando hacia módulos con puertos de tecnologías de alta velocidad.

4.3.3.1 Alternativas de diseño finales

En resumen, al momento se han determinado dos alternativas, cuya única diferencia está en el tipo de tecnología a utilizar en los segmentos de piso hacia usuarios:

La primera alternativa plantea:

a. Conmutadores seleccionados como dispositivos de conectividad tanto para el concentrador principal como para los concentradores secundarios.

b. Utilización de tecnologías de alta velocidad en todos los conmutadores (esto implica la migración de todas las interfaces de red de las estaciones de trabajo hacia tecnologías de alta velocidad).

La segunda alternativa plantea:

a. Conmutadores seleccionados como dispositivos de conectividad tanto para el concentrador principal como para los concentradores secundarios.
b. Utilización de tecnologías de alta velocidad en el conmutador principal (centro del *backbone*) y en el conmutador de servidores. Para los conmutadores de segmentos de usuarios se plantea la utilización de tecnologías tradicionales (10 Base T específicamente).

La figura 4.5 presenta la configuración en cuanto a dispositivos de conectividad definitiva, en la que se determinó que sean conmutadores los equipos de conectividad a utilizarse en todos los segmentos.

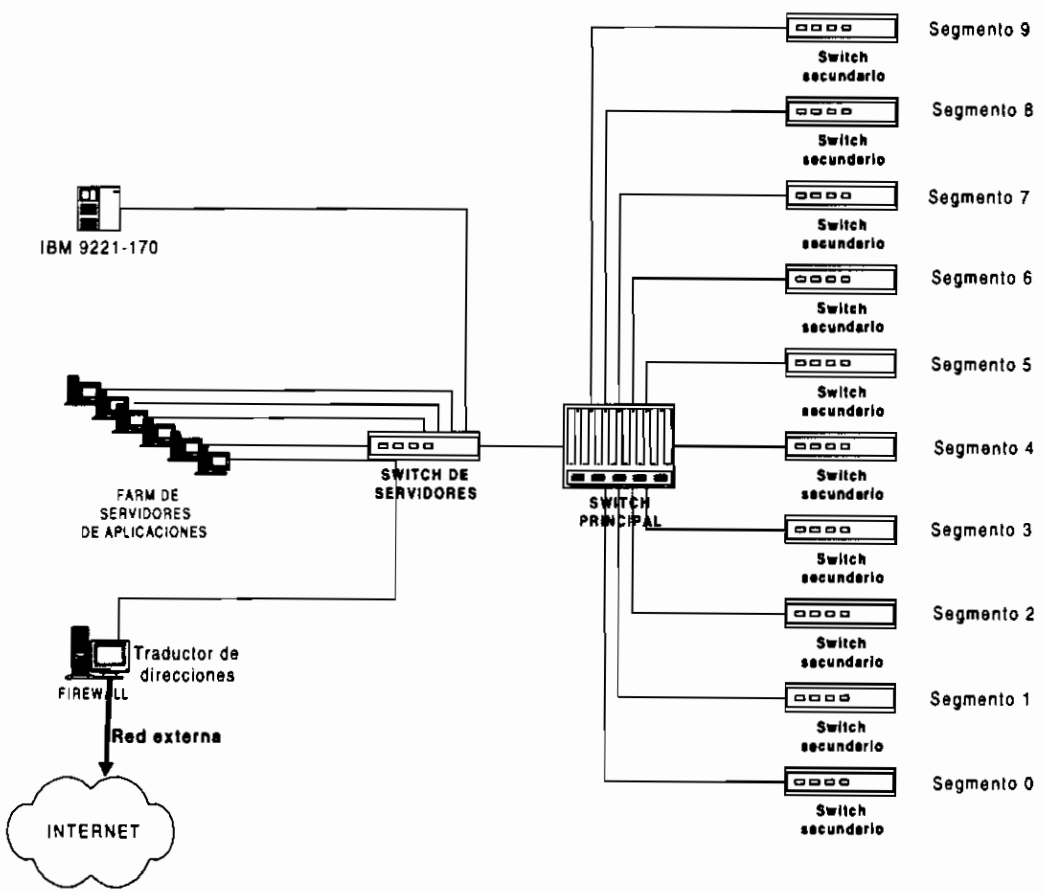


Figura 4.5 Diseño de subsistema de conectividad que plantea la utilización de conmutadores (*switches*) en todos sus segmentos

4.3.3.2 Selección de tecnologías a utilizar en alternativas finales

En las dos alternativas finales propuestas, queda por determinar el tipo de tecnología de alta velocidad que debe utilizarse en el *switch* principal y *switch* de servidores.

Adicionalmente, en la primera alternativa está pendiente determinar el tipo de tecnología de alta velocidad que deben utilizar los conmutadores o *switches* secundarios.

Para la segunda alternativa, ya se eligió a *Ethernet* 10BaseT como tecnología tradicional para ser utilizada en los *switches* secundarios.

Para la determinación de tecnologías a utilizar en cada segmento, en la tabla 4.10 se pueden ver las posibles combinaciones que se tienen para el *switch* principal, *switch* de servidores y *switches* secundarios.

1.	*Fast Ethernet* (10/20/100/200 *autosensing*)	*Fast Ethernet* (100/200 Mbps)	*a. Ethernet 10BaseT* *b. Fast Ethernet (10/20/100/200 autosensing)*
2.	*Fast Ethernet* (10/20/100/200 *autosensing*)	FDDI (100 Mbps)	*a. Ethernet 10BaseT* *b. Fast Ethernet (10/20/100/200 autosensing)*
3.	*Fast Ethernet* (10/20/100/200 *autosensing*)	ATM (155 Mbps)	*a. Ethernet 10BaseT* *b. Fast Ethernet (10/20/100/200 autosensing)*
4.	*Fast Ethernet* (10/20/100/200 *autosensing*)	Gigabit *Ethernet*	*a. Ethernet 10BaseT* *b. Fast Ethernet (10/20/100/200 autosensing)*
5.	ATM (25 Mbps)	ATM (155 Mbps)	*a. Ethernet 10BaseT* *b. Fast Ethernet (10/20/100/200 autosensing)* *c. ATM (25 Mbps)*
6.	ATM (155 Mbps)	ATM (155 Mbps)	*a. Ethernet 10BaseT* *b. Fast Ethernet (10/20/100/200 autosensing)* *c. ATM (25 Mbps)* *d. ATM (155 Mbps)*

***Tabla 4.10* Posibles combinaciones de tecnologías a utilizar**

La forma en que debe interpretarse la tabla 4.10 es la siguiente: cada numeral de la primera columna (del 1 al 6) puede combinarse con cualquier literal de la columna 4 (a b, c ó d). Los numerales indican la selección de tecnologías para el *switch* de servidores y el *switch* principal (de *backbone*), es decir para la combinación de la

segunda y tercera columna. Los literales indican las tecnologías disponibles que pueden utilizarse en los *switches* secundarios a los que se conectan las estaciones de trabajo, es decir las opciones presentadas en la cuarta columna (a, b, c ó d).

Por ejemplo, la combinación 5.b significaría la utilización de ATM (25 Mbps) para los servidores hacia el *switch* de servidores, ATM (155 Mbps) para el *switch* principal (*backbone*) y ATM (25 Mbps) entre los *switches* secundarios y las estaciones de trabajo.

En la tabla 4.11 se muestran las ventajas y desventajas de las combinaciones correspondientes a la tabla 4.10.

Numeral	Ventajas	Desventajas
1	**Para a. y b.** • Excelente manejo de tráfico no isocrónico en *backbone* y servidores • Uso de tecnología madura • Servidores pueden utilizar tarjetas de 10 ó 100 Mbps y el doble en modo full dúplex • Tráfico homogéneo (sólo conmutación paquetes)	**Para a. y b.** • El método de acceso CSMA/CD es no determinístico, lo que no es conveniente para tráfico de tipo isocrónico
	Para a. • Excelente manejo de tráfico no isocrónico en estaciones • Estaciones pueden utilizar tarjetas de 10 Mbps existentes	**Para a.** • Velocidad de 10 Mbps en estaciones para altas exigencias de tráfico isocrónico podría resultar insuficiente
	Para b. • Excelente manejo de tráfico no isocrónico y buen manejo de tráfico isocrónico cuando se utilizan 100/200 Mbps en estaciones • Estaciones pueden utilizar tarjetas de 10 ó 100 Mbps y el doble en modo full dúplex • Facilita proceso de migración (primero con 10 Mbps y luego hacia 100 Mbps)	**Para b.** • Seguir manteniendo tarjetas de 10 Mbps en estaciones para altas exigencias de tráfico isocrónico podría resultar insuficiente. Se debe notar que en esta alternativa ya pueden utilizarse tarjetas *Fast Ethernet*.
2	**Para a. y b.** • Buen manejo de tráfico no isocrónico • Servidores pueden utilizar tarjetas de 10 ó 100 Mbps y el doble en modo full dúplex • *Backbone* posee tolerancia a fallas por el doble anillo de FDDI • Método de acceso *token* en el *backbone* FDDI es determinístico, lo que favorece al tratarse de tráfico isocrónico	**Para a. y b.** • FDDI es un protocolo no escalable • FDDI podría requerir segmentación de paquetes cuando los transmite hacia los segmentos *Ethernet* (longitudes máximas de paquetes diferentes)
	Para a. • Excelente manejo de tráfico no isocrónico en estaciones • Estaciones pueden utilizar tarjetas de 10 Mbps existentes	**Para a.** • Velocidad de 10 Mbps en estaciones para altas exigencias de tráfico isocrónico podría resultar insuficiente
	Para b. • Excelente manejo de tráfico no isocrónico y buen manejo de tráfico isocrónico cuando se utilizan 100/200 Mbps en estaciones • Estaciones pueden utilizar tarjetas de 10 ó 100 Mbps y el doble en modo full dúplex • Facilita proceso de migración (primero con 10 Mbps y luego hacia 100 Mbps)	**Para b.** • Seguir manteniendo tarjetas de 10 Mbps en estaciones para altas exigencias de tráfico isocrónico podría resultar insuficiente. Se debe notar que en esta alternativa ya pueden utilizarse tarjetas *Fast Ethernet*.
3	**Para a. y b.** • Servidores pueden utilizar tarjetas de 10 ó 100 Mbps y el doble en modo full dúplex • *Backbone* está listo para transmitir cualquier tipo de tráfico (isocrónico y no isocrónico)	**Para a. y b.** • El tráfico no es homogéneo en el ambiente (se tiene la combinación de celdas y paquetes)

	Para a. • Excelente manejo de tráfico no isocrónico en estaciones • Estaciones pueden utilizar tarjetas de 10 Mbps existentes	**Para a.** • Velocidad de 10 Mbps en estaciones para altas exigencias de tráfico isocrónico podría resultar insuficiente
	Para b. • Excelente manejo de tráfico no isocrónico y buen manejo de tráfico isocrónico cuando se utilizan 100/200 Mbps en estaciones • Estaciones pueden utilizar tarjetas de 10 ó 100 Mbps y el doble en modo full dúplex • Facilita proceso de migración (primero con 10 Mbps y luego hacia 100 Mbps)	**Para b.** • Seguir manteniendo tarjetas de 10 Mbps en estaciones para altas exigencias de tráfico isocrónico podría resultar insuficiente. Se debe notar que en esta alternativa ya pueden utilizarse tarjetas *Fast Ethernet*.
4	**Para a. y b.** • Servidores pueden utilizar tarjetas de 10 ó 100 Mbps y el doble en modo full dúplex • Por la capacidad de transmisión del *backbone* (1×10^9 Mbps), se presume un buen manejo de cualquier tipo de tráfico • Se tiene un tráfico homogéneo (sólo paquetes)	**Para a. y b.** • El método de acceso CSMA/CD es no determinístico, lo que no es conveniente para tráfico de tipo isocrónico • La tecnología Gigabit *Ethernet* es relativamente nueva, aunque está fundamentalmente basada en tecnología probada pero con velocidades mucho mayores
	Para a. • Excelente manejo de tráfico no isocrónico en estaciones • Estaciones pueden utilizar tarjetas de 10 Mbps existentes	**Para a.** • Velocidad de 10 Mbps en estaciones para altas exigencias de tráfico isocrónico podría resultar insuficiente
	Para b. • Excelente manejo de tráfico no isocrónico y buen manejo de tráfico isocrónico cuando se utilizan 100/200 Mbps en estaciones • Estaciones pueden utilizar tarjetas de 10 ó 100 Mbps y el doble en modo full dúplex • Facilita proceso de migración (primero con 10 Mbps y luego hacia 100 Mbps)	**Para b.** • Seguir manteniendo tarjetas de 10 Mbps en estaciones para altas exigencias de tráfico isocrónico podría resultar insuficiente. Se debe notar que en esta alternativa ya pueden utilizarse tarjetas *Fast Ethernet*.
5	**Para a., b. y c.** • Excelente manejo de tráfico isocrónico y no isocrónico en *backbone* y servidores • Se tiene un tráfico homogéneo (sólo celdas) en *backbone* y servidores	**Para a., b. y c.** • Requiere adquisición de tarjetas de red ATM en los servidores manteniendo una velocidad limitada a 25 Mbps
	Para a. • Excelente manejo de tráfico no isocrónico en estaciones • Estaciones pueden utilizar tarjetas de 10 Mbps existentes	**Para a.** • Velocidad de 10 Mbps en estaciones para altas exigencias de tráfico isocrónico podría resultar insuficiente
	Para b. • Excelente manejo de tráfico no isocrónico y buen manejo de tráfico isocrónico cuando se utilizan 100/200 Mbps en estaciones • Estaciones pueden utilizar tarjetas de 10 ó 100 Mbps y el doble en modo full dúplex • Facilita proceso de migración (primero con 10 Mbps y luego hacia 100 Mbps)	**Para b.** • Seguir manteniendo tarjetas de 10 Mbps en estaciones para altas exigencias de tráfico isocrónico podría resultar insuficiente. Se debe notar que en esta alternativa ya pueden utilizarse tarjetas *Fast Ethernet*.
	Para c. • En este numeral (5.), y con tecnología ATM incluida hasta las estaciones de trabajo, se conseguiría tráfico homogéneo (conmutación de celdas) • Capacidad de manejo de cualquier tipo de tráfico	**Para c.** • La configuración actual requiere la compra de interfaces ATM de 25 Mbps para todas las estaciones de trabajo

6	**Para a., b. y c.** • Excelente manejo de tráfico isocrónico y no isocrónico en *backbone* y servidores • Se tiene un tráfico homogéneo (sólo celdas) en *backbone* y servidores • Velocidad en servidores de 155 Mbps por puerto	**Para a., b. y c.** • Requiere adquisición de tarjetas de red ATM de 155 Mbps en los servidores
	Para a. • Excelente manejo de tráfico no isocrónico en estaciones • Estaciones pueden utilizar tarjetas de 10 Mbps existentes	**Para a.** • Velocidad de 10 Mbps en estaciones para altas exigencias de tráfico isocrónico podría resultar insuficiente
	Para b. • Excelente manejo de tráfico no isocrónico y buen manejo de tráfico isocrónico cuando se utilizan 100/200 Mbps en estaciones • Estaciones pueden utilizar tarjetas de 10 ó 100 Mbps y el doble en modo full dúplex • Facilita proceso de migración (primero con 10 Mbps y luego hacia 100 Mbps)	**Para b.** • Seguir manteniendo tarjetas de 10 Mbps en estaciones para altas exigencias de tráfico isocrónico podría resultar insuficiente. Se debe notar que en esta alternativa ya pueden utilizarse tarjetas *Fast Ethernet*.
	Para c. • En este numeral (6.), y con tecnología ATM incluida hasta las estaciones de trabajo, se conseguiría tráfico homogéneo (conmutación de celdas) • Capacidad de manejo de cualquier tipo de tráfico y de tasas extremadamente altas	**Para c.** • La configuración actual requiere la compra de interfaces ATM de 155 Mbps para todas las estaciones de trabajo

Tabla 4.11 Ventajas y desventajas de las posibles alternativas a utilizar en la red de la figura 4.5

Resulta difícil determinar la alternativa más óptima, en función de las ventajas y desventajas de las alternativas solución que se presentan en la tabla 4.11. De hecho, resultaría fácil el escoger la alternativa que involucre las tecnologías con mayor capacidad de manejo de tráfico, y con mejores características en cuanto al manejo de cualquier tipo de tráfico. Sin embargo, antes de la selección deberían contestarse algunas preguntas:

- ¿Es necesario al momento implementar una red de esas características?
- ¿Cuánto costaría la implementación de una red de esas características?
- ¿Qué tan conveniente resultaría la implementación de una red que utilice tecnologías que permitan una inversión inicial relativamente baja, y según las necesidades que se presenten ir migrando hacia la tecnología que mejores características presente?
- ¿Es posible una combinación de las alternativas mencionadas, utilizando un proceso de migración?

Debe indicarse que todas las alternativas finalistas son técnicamente justificables de implementar, sin embargo, del análisis de inversión realizado en el capítulo V de esta tesis, se concluye que la alternativa que mejor cumple con las expectativas técnicas y económicas planteadas es la 6.b.

4.3.4 PROCESO DE MIGRACIÓN DE LA ALTERNATIVA SELECCIONADA

La alternativa seleccionada como la mejor es la alternativa 6.b, es decir un comutador principal ATM de 155 Mbps (como centro del *backbone*), un conmutador de

servidores ATM de 155 Mbps con *uplink* ATM también de 155 Mbps, y conmutadores secundarios 100BaseT (*autosensing* 10/100) hacia las estaciones de trabajo y *uplink* ATM de 155 Mbps hacia el conmutador principal.

La selección de la alternativa 6.b, facilita el proceso de migración en la porción destinada a estaciones de trabajo, pues al tener la posibilidad de seguir trabajando con 10 Mbps no se requiere el cambio inmediato de tarjetas en la mayoría de estaciones de trabajo, excepto en aquellas que son *Token-Ring*.

Un aspecto que es importante considerar es que se dispone de dos infraestructuras de transporte: una no estructurada (la de uso actual), y una estructurada (la que se utilizará en adelante), esto facilita la posibilidad de trabajar en paralelo durante el proceso de migración.

El proceso de migración en resumen se puntualiza a continuación:

- Instalación física de los equipos en los cuartos de equipamiento (MDF y SDFs – distribuidor principal o de edificio y distribuidores secundarios o de piso respectivamente) donde se dispone de la nueva infraestructura de transporte estructurada
- Conectorización de la nueva infraestructura de transporte hacia los dispositivos de conectividad mediante la utilización de *patch cords* en los MDF y SDFs. Nótese que en el lado de las estaciones de trabajo no se han realizado nuevas conexiones hasta el momento
- Pruebas de funcionamiento de equipos de conectividad (conmutadores) mediante la utilización de estaciones de trabajo y servidores de prueba, simulando la configuración futura real
- Pruebas de aplanamiento de red IP en la red actualmente utilizada
- Aplanamiento de la red IP en la red actualmente utilizada
- Conexión del subsistema de conectividad actual al nuevo subsistema de conectividad, utilizando un puerto *Token-Ring* del ruteador de uso actual con un puerto *Token-Ring* del nuevo conmutador principal.
- Conexión de las estaciones de trabajo y servidores a los nuevos conmutadores secundarios utilizando los *patch cords* y rosetas en estaciones de trabajo. Se debe indicar que este paso puede ser realizado paulatinamente usuario por usuario y segmento por segmento, hasta garantizar un buen funcionamiento mientras paralelamente sigue trabajando el sistema anterior. Este procedimiento no puede realizarse en los segmentos 4 y 6 que son *Token-Ring*, hasta que en las estaciones de trabajo se cambien las tarjetas a *Ethernet*.
- Cambio de tarjetas de red a *Ethernet* 100baseT ó 10BaseT (dependiendo de la capacidad de inversión inicial) en los segmentos *Token-Ring* 4 y 6, y conexión a los nuevos conmutadores secundarios. Nótese que este cambio también puede ir realizándose paulatinamente, mientras se mantiene la funcionabilidad del sistema antiguo.
- Se debe observar que hasta el momento, los servidores han sido conectados en los conmutadores secundarios, manteniendo el esquema actual de

servidores departamentales. Es decir, no se ha utilizado hasta el momento el conmutador ATM de servidores. Es en este paso, en el que se comienza la migración de los servidores 10/100BaseT hacia el segmento ATM 155 Mbps de servidores. Este procedimiento debe hacerse servidor por servidor, y en horas que estén fuera del funcionamiento normal de la institución, pues son cambios que afectan a grandes grupos de usuarios que hacen uso de este recurso.

- Terminada la migración de servidores y estaciones al nuevo sistema, pueden desconectarse los 2 sistemas en el segmento *Token-Ring* utilizado para ese efecto.
- En el nuevo sistema, deben empezar a definirse las redes virtuales necesarias para evitar la inundación de tráfico *broadcast* y *multicast* generado por tráfico de redes planas (IP e IPX).
- Finalmente, aunque siendo ya un proceso que involucra un trabajo más detenido sobre los servidores y estaciones de trabajo, debe empezar a eliminarse el *stack* de protocolos IPX/SPX de la red.

4.4 CARACTERÍSTICAS Y ESPECIFICACIONES TÉCNICAS DE LOS ELEMENTOS DEL SUBSISTEMA DE CONECTIVIDAD SELECCIONADO

4.4.1 CONMUTADOR PRINCIPAL

El conmutador principal seleccionado tiene las siguientes partes:

- Chasis (incluidas fuente de poder principal y fuente de poder redundante)
- Módulo de conmutación ATM
- Módulo de conmutación MicroLAN *Token-Ring*
- Módulo de acceso ATM

Cada parte es detallada en cantidad y especificaciones a continuación.

4.4.1.1 Chasis

Este chasis deberá ser un dispositivo totalmente pasivo. Es decir no deberá incluir elementos activos, tales como circuitos integrados en su parte electrónica, con el objeto de eliminar posibles puntos de falla que afecten al sistema entero.

El chasis del conmutador principal deberá soportar mínimo 8 módulos de interfaz y soportar topologías de redes mezcladas.

Con el objeto de garantizar tolerancia a fallas, el conmutador principal no debe tener un módulo de administración dedicado, sino que los módulos instalados deben comunicarse entre sí para realizar las funciones de administración del chasis. Esto permite redundancia de la administración mientras se maximiza la disponibilidad de *slots*.

Las capacidades de tolerancia a fallas del chasis del conmutador principal deberán incluirse en el sistema de poder, buses de administración, módulo de ambiente y otros componentes, para asegurar máxima disponibilidad de funcionamiento.

Adicionalmente, el chasis del conmutador principal deberá soportar todas las tecnologías de conectividad: *Ethernet*, *Token-Ring*, FDDI, ATM, SNA, y WAN, sin el uso de puentes o ruteadores externos.

A. Ambiente

El chasis deberá poseer un módulo controlador de ambiente, que permita se lleven a cabo las siguientes funciones:

- Enfriamiento del sistema
- Administración fuera de banda
- Estadísticas de las condiciones ambientales

B. *Backplane*

El *backplane* estará diseñado para conmutación de celdas y paquetes, podrá soportar cualquier tipo de conectividad LAN, WAN, SNA o ATM. Adicionalmente deberá soportar características de administración estándar de la industria SNMP.

El *backplane* debe estar compuesto por tres buses principales: bus de conmutación de paquetes, bus de conmutación de celdas y bus de administración.

De acuerdo al cálculo estimado como crítico que se realizó en el análisis cuantitativo, la capacidad del bus del conmutador central debe ser aproximadamente 1 Gbps o aproximadamente 83000 pps de 1500 bytes cada uno.

Algunos fabricantes, como CABLETRON por ejemplo, proveen este tipo de arquitectura de 3 buses (en su modelo MMAC PLUS). El primer bus (dividido en dos canales) sirve como soporte para la conmutación de paquetes, y contiene un cómodo ancho de banda (400 Mbps aproximadamente). El segundo bus (dividido en dos canales) provee soporte para conmutación de celdas, y pone a disposición un ancho de banda más alto (aproximadamente 4 Gbps). Finalmente, provee un tercer bus (también dividido en 2 canales) que sirve para que los dispositivos conectados en el chasis puedan comunicarse entre sí para cambiar información de estado, de ambiente, de mensajes de diagnóstico, comunicación entre módulos y sincronización de la administración del chasis. CABLETRON adicionalmente promete proveer un componente basado en la conmutación de celdas pero con arquitectura matricial, que permitirá una capacidad de conmutación de 60 Gbps.

De acuerdo con esto, sólo[49] el bus de conmutación de celdas del modelo MMAC PLUS de CABLETRON estaría en la posibilidad de soportar la condición crítica estimada de tráfico de la institución hipotética planteada. Es decir, los módulos a los que se conecten los cables de los conmutadores secundarios, deben estar conectados al bus de conmutación de paquetes.

C. Sistema de poder

El sistema de poder en lo posible debe generar dos voltajes de polarización (DC). El primero destinado a la polarización de módulos y dispositivos instalados en el chasis, y el segundo independiente destinado para diagnóstico de controladores utilizados sobre cada módulo.

D. Módulo de fuente de poder AC

Deberá soportar características de redundancia. Además las fuentes instaladas deberán compartir la carga durante el funcionamiento normal con el fin de prolongar el tiempo de vida de las fuentes. Adicionalmente soportarán rangos de voltaje de entrada entre 100 y 250 VAC a frecuencias de entre 50 y 60 Hz. La potencia de las fuentes será suficiente para soportar la carga más crítica del equipo (normalmente las fuentes de este tipo de equipos generan aproximadamente 1000 *watts*).

Debe poseer un sistema que genere información de estado, ambiente y diagnóstico (con estadísticas) al sistema de administración.

Finalmente las fuentes del chasis deberán estar en la capacidad de ser reemplazadas en "caliente", es decir sin la necesidad de que el equipo sea apagado.

E. Módulo de fuente de poder DC y baterías de emergencia

En lo posible, el chasis deberá tener la posibilidad de soportar un módulo que permita conectar el chasis a un voltaje DC directamente. Adicionalmente, debería tener la posibilidad de conectarse con un banco de baterías de emergencia en caso de no disponer de UPS.

F. Especificaciones estándares

Dimensiones: montable en rack de 19''
Temperatura de operación: 5 a 40° C
Humedad relativa: 5% a 95% no condensada

[49] Notar que la exclusión realizada es entre los buses del backplane del modelo MMAC PLUS que se citó como ejemplo. La exclusión no se refiere a los buses provistos por otros fabricantes.

Seguridad[50]: debe cumplir con requerimientos de seguridad de UL1950, CSA C22.2 No 950, EN 60950 e IEC950; requerimientos EMI de FCC clase A y EN 55022 clase A, VCCI clase I y los requerimientos de EN 50082-1.

4.4.1.2 Módulo de conmutación ATM

El módulo de conmutación ATM debe entregar conectividad ATM a un grupo LAN, *backbone* y aplicaciones WAN. Este módulo debe cumplir totalmente con las especificaciones ATM Forum UNI, incluyendo señalización SVC (*Switched Virtual Circuit*) y control de flujo.

Debe proveer un ancho de banda agregado mayor a 2.5 Gbps para atender a 24 estaciones o dispositivos ATM. La conectividad debe ser provista a dispositivos ATM a velocidades de 155 Mbps y debe tener la posibilidad de crecimiento en grupos *(port trunking)* de hasta 622 Mbps, 1.2 Gbps y 2.4 Gbps.

El módulo será administrable por medio de cualquier aplicación del tipo SNMP.

La conexión del módulo al chasis será a través del bus de conmutación de celdas con capacidad de 4 Gbps.

Cada módulo deberá proveer características de establecimiento de conexión automática, enrutamiento y conmutación optimizado inteligente de circuitos virtuales permanentes, *multicast* y *broadcast*.

A. Cantidad (2)

Considerando las capacidades y requerimientos del módulo de conmutación ATM, y considerando además que el chasis elegido tiene una capacidad holgada de ancho de banda y capacidad física en número de *slots*, se propone la utilización de 2 módulos de conmutación ATM de 24 puertos con conectores de fibra ST, para que además de las conexiones de los conmutadores secundarios, se conecten a este conmutador los 18 servidores de red existentes, evitando de esta manera la necesidad de un conmutador de servidores que había sido planteado inicialmente.

B. Especificaciones

Tipo de conmutador: Multiplexación por división en el tiempo
Capacidad agregada: Superior a 2.5 Gbps
Buffers de salida: Prioridad dual
Demora de conmutación de tránsito: < 10 microsegundos
Procesador de control: Tipo Intel i960 RISC
Memoria del CPU: 16 MB

[50] El detalle del significado de las especificaciones citadas, está fuera del alcance del estudio de esta tesis, sin embargo es bueno conocer que existen.

Número de Interfaces ATM: 24 puertos (instalables en grupos de 6)
Tipo de interfaces: Single 155 Mbps SONET[51] OC3 multimodo
Tipo de conector: Fibra (conector SC)
Bus de conexión: Conexión al bus de conmutación de celdas del chasis
Estándares soportados[52]: ATM Forum UNI, IETF ATM MIB, ATM Forum LAN Emulation

Administración: vía el bus de administración del chasis (a 10 Mbps) por medio de una interfaz serial

Temperatura de operación: 5 a 40° C
Humedad relativa: 5 al 95 % no condensada

4.4.1.3 Módulo de conmutación MicroLAN *Token-Ring*

Este módulo se añadió por la necesidad de conectividad hacia algunos dispositivos *Token-Ring* (tal como el IBM 9221) y para otorgar conectividad hacia LAN antiguas sin la utilización de dispositivos adicionales, tales como puentes o ruteadores. Adicionalmente, y como se planteó en el proceso de migración, estos pórticos servirán como un medio de conexión temporal entre el actual y el nuevo subsistema de conectividad.

Este módulo debe cumplir con el estándar IEEE 802.5 y debe ser completamente compatible con *Token-Ring* de IBM. Deberá conectarse al bus de conmutación de paquetes del *backplane* del chasis.

El módulo será administrable por medio de SNMP. Cada puerto *Token-Ring* debe soportar estándares MIB de SNMP, incluyendo MIB II y RMON.

A. Cantidad (1)

Un solo módulo *Token-Ring* de 2 puertos es suficiente para satisfacer las necesidades planteadas. Sin embargo, en el mercado normalmente se encuentran módulos *Token-Ring* con un mínimo de 8 puertos.

B. Especificaciones

Capacidad de almacenamiento del Sistema operativo local: 2 MB (expandible a 14 MB)

---

[51] La serie SONET (*Synchronous Optical NETwork*) soporta transmisión de datos de alta velocidad. SONET provee soporte para muchos formatos de entrada (T1, E1, T3, *Ethernet*, ATM) para ser enviada sobre un enlace de fibra óptica. La especificación SONET OC-3 provee soporte de hasta 2 Km para una velocidad de 155 Mbps sobre fibra multimodo, y 25 Km para la misma velocidad sobre fibra monomodo.
[52] El detalle del significado de las especificaciones citadas, está fuera del alcance del estudio de esta tesis, sin embargo es bueno conocer que existen.

Procesador de control: Tipo Intel i960 RISC
Memoria del CPU: 4 MB de RAM dinámica (expandible a 12 MB)

Número de Interfaces Token-Ring: 8 puertos
Tipo de interfaces: Token-Ring (16 Mbps)
Tipo de conector: RJ-45
Bus de conexión: Conexión al bus de conmutación de paquetes del backplane del chasis
Estándares soportados: IEEE 802.5 y debe ser completamente compatible con Token-Ring de IBM

Administración: vía el bus de administración del chasis (a 10 Mbps) por medio de una interfaz serial

Temperatura de operación: 5 a 40° C
Humedad relativa: 5 al 95 % no condensada

4.4.1.4 Módulo de acceso ATM

Este módulo se hace necesario para conectar una red externa ATM al bus de conmutación de paquetes del *backplane*. Las conexiones externas son hechas por medio de un panel frontal, con interfaces SONET ATM de 155 Mbps.

El módulo de acceso ATM puede ser usado para agregar tráfico de paquetes a un *backbone* ATM, o para proveer conectividad entre estaciones ATM a usuarios de LAN tradicionales.

El módulo de acceso será compatible totalmente con especificaciones del Forum ATM, incluyendo[53] Q.2931, ILMI y LAN Emulation. Este actúa como un cliente LAN Emulation del Forum ATM, permitiendo que usuarios de LANs tradicionales (*Ethernet*, *Token-Ring*, FDDI) accesen a un *backbone* ATM.

A. Cantidad (1)

Un solo módulo de acceso ATM es necesario para proveer la conectividad del módulo *Token-Ring* al *backbone* ATM.

B. Especificaciones

Procesador de control: Tipo Intel i960 RISC
Memoria del CPU: 4 MB de RAM local (expandible a 16 MB)
4 MB de RAM compartida (expandible a 16 MB)
2 MB de memoria flash (expandible a 16 MB)

Número de Interfaces ATM: 1 puerto

[53] El detalle del significado de las especificaciones citadas, está fuera del alcance del estudio de esta tesis, sin embargo es bueno conocer que existen.

Tipo de interfaces: Single 155 Mbps SONET OC3 multimodo
Tipo de conector: Fibra (conector SC)
Bus de conexión: Conexión al bus de conmutación de paquetes del chasis

Administración: vía el bus de administración del chasis (a 10 Mbps) por medio de una interfaz serial

Temperatura de operación: 5 a 40° C
Humedad relativa: 5 al 95 % no condensada

4.4.1.5 Conexión del conmutador principal

En la figura 4.5 se muestra el esquema de conexión en el conmutador principal, entre módulos y hacia estaciones y conmutadores secundarios.

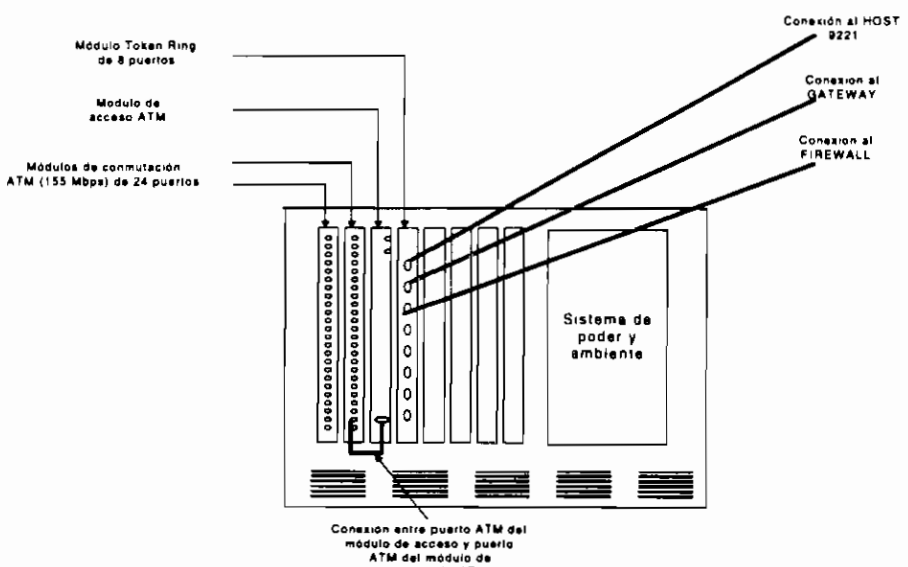


***Figura 4.5** Esquema de conexión entre módulos para el conmutador principal*

4.4.2 CONMUTADORES SECUNDARIOS

Cada conmutador secundario seleccionado tiene las siguientes partes:

- Chasis (incluidas fuente de poder principal y fuente de poder redundante)
- Módulos MicroLan *Fast Ethernet*
- Módulos MicroLan *Fast Ethernet* con interfaz de alta velocidad

4.4.2.1 Chasis

De las mismas características generales que el chasis del conmutador principal tales como:

- Chasis totalmente pasivo
- Sistema de control integrado en cada módulo que se añade al chasis, y no un módulo de control general para todos los módulos.
- Capacidades de tolerancia a fallas en el sistema de poder, buses de administración, módulo de ambiente y otros componentes
- Modularidad : para preveer la incorporación de tecnologías existentes y emergentes en un mismo dispositivo
- Protección de la inversión: para garantizar una larga vida útil del producto, actualización disponible de *firmware* y facilidad en la transición de redes tradicionales a redes virtuales.
- Ambiente, igual que en el conmutador principal
- Sistema de poder, igual que en el conmutador principal
- Módulos de fuente de poder AC y DC, igual que en el conmutador principal

Sus características específicas serán:

- *Backplane*: considerando que se conectarán aproximadamente 60 usuarios en promedio, cada uno de los cuales podría generar 1.5 Mbps en promedio aproximadamente, el *backplane* seleccionado debería soportar al menos 90 Mbps o aproximadamente 7500 pps de 1500 bytes cada uno. En lo posible tendrá tres buses: para conmutación de paquetes, circuitos y un bus para administración y control del sistema.

  En la práctica, la mayor parte de fabricantes, no diseñan sus conmutadores de este tipo de aplicación con tres buses en el *backplane*, sin embargo se manejan 2 buses, uno para datos (aproximadamente con una capacidad de manejo de 2´000.000 de paquetes por segundo o aproximadamente 3.2 Gbps) y otro para administración y control.

- Capacidad de módulos: deberá estar en la capacidad de soportar 120 puertos con soporte de RMON por puerto. Es decir, si se disponen de módulos de 24 puertos debería tener 5 *slots* disponibles para pórticos hacia estación, con una capacidad de manejo de 400.000 pps por módulo.

Cantidad (9)

Considerando que se tienen 9 segmentos principales, y considerando que la distribución de usuarios por segmento (piso) es de 60 aproximadamente, se hacen necesarios 9 chasis con 5 *slots* cada uno, y con capacidad para manejar más de 90 puertos *Fast Ethernet* (para garantizar conexión de los pisos con mayor densidad de usuarios y holgura ante futuros requerimientos).

4.4.2.2 Módulos MicroLan *Fast Ethernet*

La tecnología actual hasta el momento, provee módulos de conmutación *Fast Ethernet*, pero con la atenuante que en el chasis previsto en características y precio, sólo puede acomodar hasta 40 puertos *Fast Ethernet* conmutados. Debe notarse que el contar con una capacidad de 100 Mbps dedicados, es posiblemente exagerado para las aplicaciones que se requieren en la institución hipotética actualmente.

El chasis para el tipo de conmutador seleccionado, puede soportar más de 60 puertos *Fast Ethernet* pero con la eficiencia de *hubs* de acceso compartido por módulo. Se debe observar que cada módulo debe tener una capacidad de manejar 400.000 pps ó 640 Mbps aproximadamente. Si se considera que los módulos son de autonegociación (10/100 Mbps) las estaciones con 10 Mbps pueden seguir funcionando adecuadamente mientras se garantiza una fácil migración a *Fast Ethernet*.

Adicionalmente, con el objeto de optimizar espacio en conectorización, se requiere que los conectores sean tipo telco o RJ21 por módulo.

A. Cantidad (22)

Considerando que se tendrán aproximadamente 740 usuarios en el edificio, se considera necesario la utilización de 31 módulos de 24 puertos *Fast Ethernet*, sin embargo 9 de ellos deben poseer una conexión con una interfaz de alta velocidad (ATM 155 Mbps). Por tanto se requieren 22 módulos de 24 puertos *Fast Ethernet*.

B. Especificaciones

Procesador de control: Tipo Intel i960 RISC
Dispositivo de conmutación: (ASIC)
Memoria del CPU: 16 MB de RAM
Memoria compartida: 4 MB de RAM
Memoria FLASH: 4 MB de memoria flash

Número de Interfaces Fast Ethernet (autonegociación): 24 puertos
Tipo de interfaces: Fast Ethernet 100BaseTx (10/100)
Tipo de conector: RJ21 (cable Telco)

Administración: vía el bus de administración del chasis (a 10 Mbps) por medio de una interfaz serial para administración fuera de banda y SNMP para administración en banda

Temperatura de operación: 5 a 40° C
Humedad relativa: 5 al 95 % no condensada

4.4.2.3 Módulos MicroLan *Fast Ethernet* con interfaz de alta velocidad

Las características de estos módulos son idénticas a las del numeral 4.4.2.2, pero adicionalmente, proveen soporte para interfaces de alta velocidad. El interfaz de alta velocidad que se necesita es ATM de 155 Mbps soportado sobre fibra óptica con conector SC.

A. Cantidad (9)

Se requieren 9 módulos de este tipo, para que cada uno sea ubicado en cada chasis de conmutador secundario. El resto de pórticos en el chasis se conseguirá con la instalación de módulos *Fast Ethernet* simples.

B. Especificaciones

Procesador de control: Tipo Intel i960 RISC
Dispositivo de conmutación: (ASIC)
Memoria del CPU: 16 MB de RAM
Memoria compartida: 4 MB de RAM
Memoria FLASH: 4 MB de memoria flash

Número de Interfaces Fast Ethernet (autonegociación): 24 puertos
Tipo de interfaces: Fast Ethernet 100BaseTx (10/100)
Tipo de conector: RJ21 (cable Telco)

Número de interfaces de alta velocidad: 1
Tipo de interfaz de alta velocidad: ATM 155 Mbps
Tipo de conector: Conector SC de fibra óptica

Administración: vía el bus de administración del chasis por medio de una interfaz serial para administración fuera de banda y SNMP para administración en banda

Temperatura de operación: 5 a 40° C
Humedad relativa: 5 al 95 % no condensada

4.4.2.4 Conexión de los conmutadores secundarios

En la figura 4.6 se muestra el esquema de disposición de los módulos en el conmutador secundario.

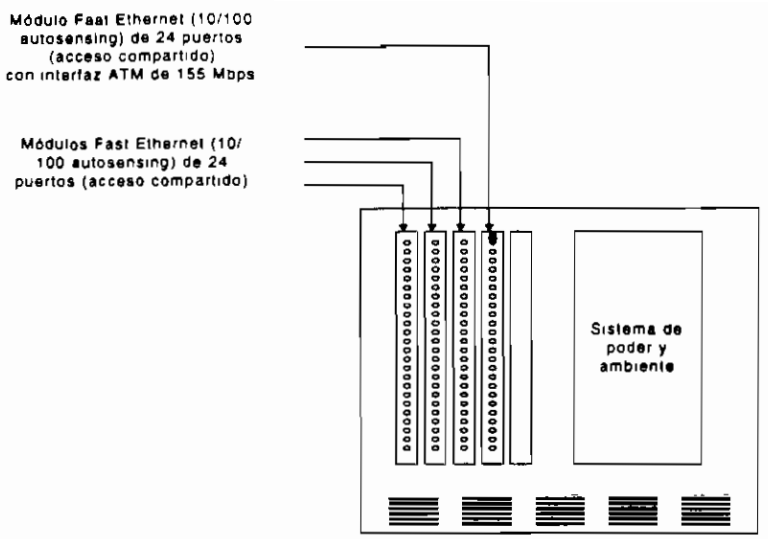


***Figura 4.6** Esquema de disposición de módulos en el conmutador secundario*

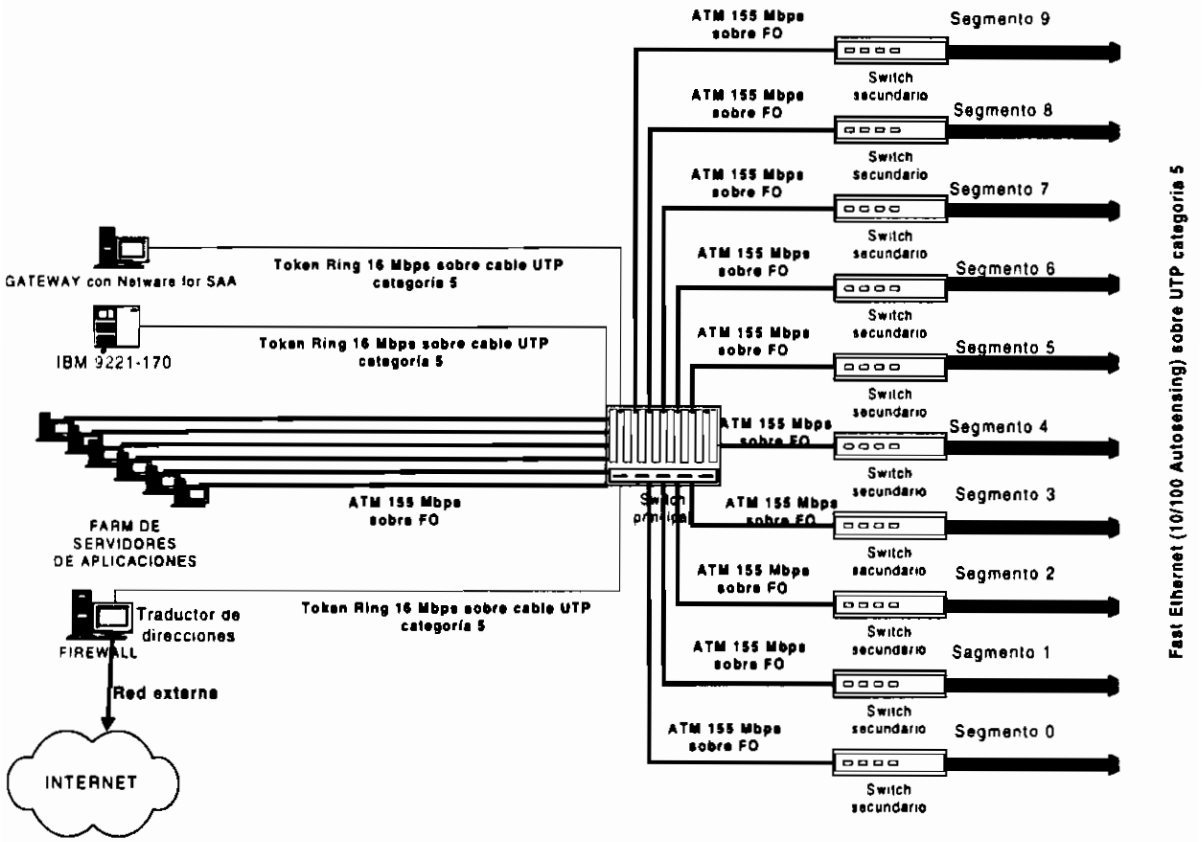


***Figura 4.7** Diseño de red definitivo*

4.4.3 CONMUTADOR DE SERVIDORES

Como se explicó en el numeral 4.4.1, la capacidad de ancho de banda y flexibilidad de crecimiento del chasis del conmutador principal, permite que los servidores se integren al conmutador principal, ahorrando de esta manera la utilización de un conmutador de servidores exclusivamente.

4.4.4 CONFIGURACIÓN DEFINITIVA

El sistema final planteado es como se muestra en la figura 4.7.

4.5 APLICACIONES FACTIBLES DE IMPLEMENTAR SOBRE EL SISTEMA PLANTEADO

Entre las aplicaciones que el sistema planteado estará en capacidad de soportar están:

- Aplicaciones de manejo archivos y conexiones remotas
  - Copias remotas
  - FTP
  - TELNET
  - HTTP
- Aplicaciones multimedia
  - Video conferencia
  - Correo electrónico de voz y video
  - Capacitación a través de la red
- Aplicaciones de flujo de documentos
  - Lotus Notus
- Aplicaciones de administración de red
  - Open View de HP
  - SPECTRUM de Cabletron
  - LAN Management de IBM
- Aplicaciones de trabajo en grupo con altas tasas de tráfico ubicados en sitios físicos lejanos en la LAN, gracias a la implementación de redes virtuales
  - Autocad

V. ANÁLISIS DE INVERSION

En el numeral 4.3.3 del capítulo IV, se planteó la necesidad de realizar un análisis de inversión de las alternativas de solución propuestas.

El propósito de este análisis consiste fundamentalmente de lo siguiente:

- Asegurar que la inversión realizada en los recursos planteados sea prudente y de costo efectivo
- Documentar los costos y beneficios de las alternativas planteadas de forma metódica
- Estimar los costos y beneficios de las alternativas sobre un ciclo de vida estimado
- Ayudar en la selección de la mejor alternativa

El análisis de inversión se realizará considerando principalmente los siguientes puntos:

- Narrativa del proyecto
- Costos de desarrollo y operación
- Costos y beneficios – tangibles e intangibles
- Valor presente y beneficio neto
- Análisis de riesgo y comparación de alternativas
- Resumen de la decisión

5.1 NARRATIVA DEL PROYECTO

La narrativa del proyecto ya ha sido desarrollada en el capítulo anterior. En resumen, se busca el mejor diseño de un subsistema de conectividad a funcionar sobre una infraestructura de transporte ya diseñada.

Se entiende que la infraestructura de transporte ha sido diseñada con los mismos objetivos del subsistema de conectividad, es decir, se busca un sistema que soporte altas cargas de tráfico tanto isocrónico como no isocrónico. Sobre esta hipótesis, se asume que los requerimientos que debe cumplir la infraestructura de transporte son satisfechos en su totalidad.

El proyecto necesita del análisis de inversión, debido a que se han presentado varias alternativas que pueden ser soluciones válidas[54]. Sin embargo, debe elegirse aquella alternativa que más se ajuste a las necesidades presentes y futuras, así como al mejor costo posible.

Debe recordarse que las alternativas propuestas son alternativas de tecnologías que serán implementadas con conmutadores (*switches*), según el modelo presentado en la figura 4.5 del capítulo anterior.

[54] Estas alternativas pueden verse en la tabla 4.10 del capítulo IV

5.2 COSTOS DE DESARROLLO Y OPERACIÓN

Los costos de desarrollo y operación incluyen todos los gastos, directos e indirectos, necesarios para desarrollar el proyecto durante su ciclo de vida estimado.

5.2.1 CICLO DE VIDA

Antes de nada, es necesario que se estime el ciclo de vida para cada alternativa. Esta estimación se presenta en la tabla 5.1.

Alternativa	Ciclo de vida estimado (en años)
1.a	5
1.b	10
2.a	5
2.b	10
3.a	5
3.b	10
4.a	5
4.b	12
5.a	5
5.b	8
5.c	6
6.a	5
6.b	12
6.c	8
6.d	14

***Tabla 5.1** Ciclo de vida estimado en años de cada alternativa propuesta*

Para la estimación del ciclo de vida se ha considerado:

- Capacidad de transmisión de la tecnología utilizada: Es obvio que el uso de tecnología de alta velocidad en todo el subsistema de conectividad determinará probablemente un mayor ciclo de vida.
- Tipo de tecnología utilizada: Probablemente, y debido a que las necesidades futuras están proyectadas a la utilización de tráfico multimedia, el uso de tecnología diseñada para manejar este tipo de tráfico, tendrá un ciclo de vida mayor.

5.2.2 COSTOS POR SERVICIOS DE PERSONAL

Dentro de estos costos, están involucrados principalmente los costos que se requeriría para la contratación de nuevo personal, si fuera necesario.

Si se considera que la entidad hipotética cuenta con personal técnico calificado, la contratación de nuevo personal posiblemente no será necesaria sino solamente durante la fase de implementación.

5.2.3 GASTOS DE SERVICIO Y REPUESTOS

Deben ser identificados los gastos por servicio y soporte necesarios para el desarrollo y operación de las alternativas que han sido presentadas.

Entre este tipo de gastos se tienen:

- *Entrenamiento y educación*, que involucra los gastos necesarios para que el personal obtenga capacitación (en el exterior) de la alternativa correspondiente. La estimación de estos gastos se ha realizado considerando que la capacitación en cada tecnología de alta velocidad valdrá 1000 dólares por persona y por curso, mientras que la capacitación en tecnología tradicional valdrá 300 dólares por persona y por curso.
- *Viajes*, que cubre costos relativos a viajes necesarios involucrados con cada alternativa. Los viajes podrían necesitarse para conocer otras implementaciones en producción, capacitación, etc. Los costos por viajes se han considera en todas las alternativas con igual valor, pues se considera que en cualquier alternativa la necesidad de viajar se presenta en la misma proporción.
- *Servicios profesionales externos*, cubren los gastos de contratistas privados.
- *Repuestos*, cubre los gastos de materiales y repuestos directamente atribuidos a cada alternativa.
- *Mantenimiento preventivo y correctivo*, incluye los gastos necesarios para una operación continua del equipo u otra maquinaria relativa al proyecto. Incluye contrato de mantenimiento que se extiende sobre la vida del recurso. No incluye la provisión de repuestos.
- *Otros*, gastos tales como preparación y mantenimiento del sitio donde estarán los equipos, utilidades (teléfono, energía eléctrica, aire acondicionado, etc.).

Un resumen de los costos de desarrollo y operación estimados se indica en la tabla 5.2.

5.3 BENEFICIOS TANGIBLES

Los beneficios tangibles son usados para cuantificar en dinero los beneficios esperados de una alternativa en particular. Debe notarse que no todos los beneficios son cuantificables, y mucho se reducirá el cálculo a la estimación. Posteriormente se identificarán los beneficios intangibles.

Costo de desarrollo y operación (USD)																		
Alternativa	Vida útil (años)	Nuevo personal durante 2 semanas para cambio de tarjetas de red			Entrenamiento y educación			Viajes			Servicios prof. por año	Servicios prof. por vida útil	Mant. por año	Mant. por vida útil	Otros gastos por año	Otros gastos por vida útil	Costo por vida útil	Costo por año
		Nro pers.	Costo por persona	Total	Nro pers.	Costo por persona	Total	Nro pers.	Costo por persona	Total								
1.a	5	2	600	1200	2	1300	2600	2	2000	4000	500	2500	2000	10000	300	1500	21800	4360
1.b	8	2	750	1500	2	1000	2000	2	2000	4000	400	3200	2000	16000	300	2400	29100	3637
2.a	5	2	600	1200	2	2300	4600	2	2000	4000	900	4500	3500	17500	300	1500	33300	6660
2.b	10	2	750	1500	2	2000	4000	2	2000	4000	800	8000	3500	35000	300	3000	55500	5550
3.a	5	2	600	1200	2	2300	4600	2	2000	4000	900	4500	3500	17500	300	1500	33300	6660
3.b	10	2	750	1500	2	2000	4000	2	2000	4000	800	8000	3500	35000	300	3000	55500	5550
4.a	5	2	600	1200	2	2300	4600	2	2000	4000	900	4500	2800	14000	300	1500	29800	5960
4.b	12	2	750	1500	2	2000	4000	2	2000	4000	800	9600	2300	27600	300	3600	50300	4191
5.a	5	2	600	1200	2	1300	2600	2	2000	4000	500	2500	2800	14000	300	1500	25800	5160
5.b	8	2	750	1500	2	2000	4000	2	2000	4000	800	6400	3000	24000	300	2400	42300	5287
5.c	6	10	900	9000	2	1000	2000	2	2000	4000	400	2400	2200	13200	300	1800	32400	5400
6.a	5	2	600	1200	2	1300	2600	2	2000	4000	500	2500	2500	12500	300	1500	24300	4860
6.b	12	2	750	1500	2	2000	4000	2	2000	4000	800	9600	2700	32400	300	3600	55100	4591
6.c	8	10	900	9000	2	1000	2000	2	2000	4000	400	3200	2200	17600	300	2400	38200	4775
6.d	14	10	900	9000	2	1000	2000	2	2000	4000	400	5600	2200	30800	300	4200	55600	3971

Tabla 5.2 Costos de desarrollo y operación

5.3.1 REDUCCIÓN DE COSTOS

Incluye los tipos de gastos que son actualmente necesarios, y que pueden ser reducidos o eliminados como un resultado de que determinada alternativa sea implementada.

a. Actualización de tecnología / año

La actualización tecnológica se hace necesaria cada determinado período de tiempo. Se ha considerado que el ahorro de actualización de tecnología debido al tiempo de vida útil estimado para cada alternativa es el resultado de la suma de costos que implicaría el actualizar los equipos de conectividad (no se incluyen costos de operación).

b. Caídas de red /año

En la entidad hipotética se estima que en cada segmento de red se pierde el servicio durante 4 horas al año. Considerando que son nueve segmentos, y que por segmento se tienen en promedio 60 estaciones trabajando simultáneamente, se obtiene que el tiempo fuera de servicio en promedio por estación por año será:

4 x 9 x 60 = 2160 horas fuera de servicio de estación / año

Considerando que en cualquier entidad productiva la mínima producción debe ser por lo menos igual al salario que se paga a los empleados, se puede estimar una producción mínima por hombre por hora de la entidad. Si se considera que un empleado que utiliza una computadora tiene un salario promedio de $ 550 al mes, y que su trabajo depende en un 80% del uso de ella, puede estimarse que la producción mínima por hora por estación de trabajo es la siguiente:

550/20/8*(0.8) = 2.75 dólares /hora-estación

De aquí se deduce que el gasto actual en caídas de red es mínimo igual a:

2.75 * 2160 = 5940 dólares /año

5.3.2 RENTAS O REEMBOLSOS

Incluye las fuentes de nuevas o adicionales rentas o reembolsos de dinero.

Lamentablemente, la institución hipotética referida no puede cobrar por los servicios que provee a otras instituciones y difícilmente se pueden cuantificar los réditos económicos que podrían cobrarse al dar un servicio más eficiente. Esta deficiencia es pagada a cambio de la imagen que guardará la institución al brindar un mejor servicio.

5.3.3 HORAS DE TRABAJO AHORRADAS A LA INSTITUCIÓN

Incluye el tiempo ahorrado en trabajo u horas desperdiciadas a la institución.

Tiempo de respuesta de aplicaciones / año

Considerando que la producción mínima de la red por hora-red vendrá dada en función de las 741 estaciones de trabajo que se consideran en la red hipotética y del costo por hora-estación, se tendrá:

2.75 * 741 = 2037.75 dólares / hora-red

Si se toma en cuenta que el tiempo de respuesta en el trabajo de usuario mejorará en 1 hora por bisemana (estimación pesimista) por estación de trabajo, se tendrá que para un año de 26 bisemanas, el ahorro en tiempo ganado para la institución hipotética será:

2037.75 * 26 = 52981.5 dólares / año

5.3.4 SUPOSICIONES

Se debe notar que se considera una producción mínima por estación igual al salario promedio de un usuario de la mencionada estación de trabajo. Esta estimación es bastante pesimista si se considera que una entidad productiva deberá tener utilidad neta incluso descontando la cantidad destinada a salarios.

Adicionalmente se considera que el ahorro en tiempo de trabajo se mejora por usuario tan solo en 1 hora por bisemana, es decir media hora semanal.

La cuantificación de los beneficios tangibles se detalla en la tabla 5.3.

5.4 COSTOS Y BENEFICIOS INTANGIBLES

Los costos y beneficios intangibles son utilizados para describir costos y beneficios difíciles de cuantificar en términos de dinero. Los beneficios intangibles son expresados frecuentemente en términos de qué cosa hace mejor.

Es conveniente utilizar listas donde se describan brevemente los beneficios y costos intangibles de cada alternativa, y listas de quienes son afectados por esos beneficios o costos.

La evaluación estimada de estos costos y beneficios es mostrada en la tabla 5.4. Nótese que la evaluación se hace sobre un valor máximo de 10, considerando que cualquier valor sobre 5 puede considerarse como un beneficio intangible, mientras que cualquier valor bajo 5 puede considerarse como un costo intangible.

	Alternativas														
	1.a	*1.b*	*2.a*	*2.b*	*3.a*	*3.b*	*4.a*	*4.b*	*5.a*	*5.b*	*5.c*	*6.a*	*6.b*	*6.c*	*6.d*
Beneficios Tangibles															
Reducción de costos															
Actualización de tecnología / año	0	29740	0	29740	0	29740	0	29740	0	29740	45416.66667	0	29740	45416.66667	145980
Caídas de red /año	5940	5940	5940	5940	5940	5940	5940	5940	5940	5940	5940	5940	5940	5940	5940
Rentas o reembolsos															
	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
Horas de trabajo ahorradas a la institución															
Tiempo de respuesta de aplicaciones / año	52981.5	52981.5	52981.5	52981.5	52981.5	52981.5	52981.5	52981.5	52981.5	52981.5	52981.5	52981.5	52981.5	52981.5	52981.5
Beneficios tangibles por año	*58921.5*	*88661.5*	*58921.5*	*88661.5*	*58921.5*	*88661.5*	*58921.5*	*88661.5*	*58921.5*	*88661.5*	*104338.1667*	*58921.5*	*88661.5*	*104338.1667*	*204901.5*
Vida útil	*5*	*8*	*5*	*10*	*5*	*10*	*5*	*12*	*5*	*8*	*6*	*5*	*12*	*8*	*14*
Total durante vida útil	*294607.5*	*709292*	*294607.5*	*886615*	*294607.5*	*886615*	*294607.5*	*1063938*	*294607.5*	*709292*	*626029*	*294607.5*	*1063938*	*834705.3333*	*2868621*

Tabla 5.3 Beneficios tangibles

	Alternativas (puntaje entre 1 y 10)														
	1.a	*1.b*	*2.a*	*2.b*	*3.a*	*3.b*	*4.a*	*4.b*	*5.a*	*5.b*	*5.c*	*6.a*	*6.b*	*6.c*	*6.d*
Costos y Beneficios intangibles															
Generales															
Imagen institucional	6	7	6	7	7	8.5	8	9	7	8.5	8	7.5	9	8.5	9.5
Impacto sobre usuarios en la tecnología y por tanto mejor desempeño	7	7.5	7	8.5	7	8.5	7	8.5	7	8.5	8	7	9	8	9
Vida útil proyectada (valorando como 10 al máx.)	3.6	5.8	3.6	7.2	3.6	7.2	3.6	8.6	3.6	5.8	4.3	3.6	8.6	5.8	10
Técnicos															
Manejo de tráfico no isocrónico	8	9	8.2	9.3	8	9	9	9.8	8	9	8.5	8	9	8.5	9.5
Manejo de tráfico isocrónico	6	6.5	6.2	8.2	6	8	6	8	7	7	7.5	7.5	8.5	9	9.8
Uso de tecnología madura	9	9	9	9	8	8	8.5	8.5	8	8	7.5	8	8	7.8	7.8
Homogenidad de tráfico	8.5	9.5	7	8	7	8	8	9	7.5	8	9	8	8	9	9.5
Facilidad en proceso de migración	9	9.5	9	9.5	9	9.5	9	9.5	9	9.5	7	9	9.5	7	7
Escalabilidad	8	8	7	8	7.5	8.5	8	8	7.5	8	8	8.5	9	9	9.5
Capacidad de transmisión	8	9	8	9	8	9	8.5	9.5	7.5	8.5	8	7.5	9	8.5	9.5
Ancho de banda efectivo y calidad de servicio	4	4	4.5	4.5	5	5	4.5	4.5	7	7	9	7	7	9	9
Proyección de conectividad hacia WAN	5	5	5	5	9.5	9.5	5	5	9.5	9.5	9.5	9.5	9.5	9.5	9.5
Evaluatorios (del capítulo 3)															
Conectividad	9	9	8	8	8	8	9	9	8	8	9	7.5	8	9	9.5
Flexibilidad	7	8.5	7	8	7	8.5	8.5	8.5	7	8.5	8	8	9	9	9
Compatibilidad	9.5	9.5	9.5	9.5	8	9.5	9.5	9.5	8	7.5	8	8	7.5	8	8
Disponibilidad	9.8	9.8	9.8	9.8	9.3	9.3	9.6	9.6	9.3	9.3	9.2	9.3	9.3	9.2	9.1
Capacidad (*)															
Modularidad (*)															
Productividad (*)															
(*) Estos parámetros ya se han evaluado en puntualizaciones anteriores															
Total promedio	***7.4***	***8***	***7.2***	***8.1***	***7.4***	***8.4***	***7.7***	***8.5***	***7.6***	***8.2***	***8.1***	***7.8***	***8.7***	***8.5***	***9.1***
Indice del beneficio-costo intangibles respecto al máx.	0.81	0.88	0.79	0.89	0.81	0.92	0.85	0.93	0.84	0.90	0.89	0.86	0.96	0.93	1

Tabla 5.4 Costos y Beneficios intangibles

5.5 VALOR PRESENTE Y BENEFICIO NETO

Para este efecto debe elegirse una tasa de interés que más se acerque a las condiciones de evaluación para el costo de capital o tasa actual de inflación.

Para el presente análisis se ha considerado una tasa de interés anual del 10%, pues el cálculo se hace en dólares de los EEUU.

Los datos entrantes para el cálculo del valor presente son:

- Tiempo estimado de vida útil
- Costo de equipamiento (en USD americanos). Estos costos, mostrados en la tercera columna de la tabla 5.11, se recogen de los resultados obtenidos en las tablas 5.5, 5.6, 5.7, 5.8, 5.9 y 5.10, que corresponden a los costos de equipamiento de las alternativas 1 (a y b), 2 (a y b), 3 (a y b), 4 (a y b), 5 (a, b y c) y 6 (a, b, c y d) respectivamente.
- Costos de desarrollo y operación durante el período de vida útil. Estos costos se recogen de los resultados obtenidos en la tabla 5.2.
- Beneficios tangibles durante el período de vida útil. Estos costos se recogen de los resultados obtenidos en la tabla 5.3.

El cálculo del valor presente se lo realiza primeramente obteniendo la resta de los beneficios totales menos los costos totales. A este resultado se le aplica la fórmula del valor presente, considerando una tasa de interés del 10% anual, y el período de análisis correspondiente al tiempo de vida útil estimado.

La fórmula del valor presente se muestra a continuación:

$$\text{Valor Presente} = (\text{Total beneficios} - \text{costos}) / (1 + r)^t$$

donde:

r = tasa de interés anual
t = tiempo de vida útil estimado

El cálculo del valor presente y beneficio neto se muestra en la tabla 5.11.

La columna titulada índice del valor presente respecto al máximo, es simplemente una manera diferente de cuantificar el valor presente. Para esto, se asigna el valor de 1 al máximo valor presente calculado, y el resto tendrán el valor porcentual correspondiente. De esta forma se puede visualizar con más facilidad la alternativa que mejor calificación posee.

5.6 ANALISIS DEL RIESGO

Este análisis está diseñado para medir el riesgo potencial asociado con una alternativa en particular. Requiere una respuesta numérica, en una escala del 1 al 10, a algunas preguntas relacionadas con riesgos económicos, operacionales y técnicos.

Elementos	Cantidad	Precio Unitario USD	Precio total USD	
SWITCH PRINCIPAL				
Chasis con 3 backplanes independientes con capacidad para 8 módulos	1	5500	5500	
Fuente de poder principal	1	1900	1900	
Fuente de poder redundante	1	1500	1500	
Módulo de administración del procesador	1	10000	10000	
Módulo Fast Ethernet (100/200 Mbps) de 12 puertos para FO	1	7000	7000	
			SUBTOTAL	**25900**
SWITCH DE SERVIDORES				
Chasis con 1 backplane con capacidad para 5 módulos	1	4000	4000	
Fuente de poder principal	1	1900	1900	
Fuente de poder redundante	1	1500	1500	
Módulo de administración del procesador	1	10000	10000	
Uplink 100 Base FX	1	575	575	
Módulo Fast Ethernet (10/20/100/200 Mbps autosensing) de 8 puertos de FO	2	6000	12000	
Módulo Token Ring (16 Mbps) de 8 puertos	1	4000	4000	
			SUBTOTAL	**33975**
SWITCHES SECUNDARIOS				
Chasis con 1 backplane con capacidad para 5 módulos	9	4000	36000	
Fuente de poder principal	9	1900	17100	
Fuente de poder redundante	9	1500	13500	
Módulo de administración del procesador	1	10000	10000	
Uplink 100 Base FX	9	575	5175	
a. Módulo Ethernet 10 Mbps de 24 puertos	31	7000	217000	
b. Módulo Fast Ethernet (10/20/100/200 Mbps autosensing) de 24 puertos	31	12000	372000	
			SUBTOTAL a.	**298775**
			SUBTOTAL b.	**453775**
INTERFACES DE RED				
Para servidores				
Fast Ethernet (100/200 Mbps)	12	150	1800	
Para estaciones				
a. Ethernet 10BaseT (4to y 6to pisos)	166	60	9960	
b. Fast Ethernet 100/200 Mbps (Todas las estaciones de trabajo)	741	100	74100	
			SUBTOTAL a.	**11760**
			SUBTOTAL b.	**75900**
			TOTAL 1.a	**370410**
			TOTAL 1.b	**589550**

Tabla 5.5 Costo de equipamiento de las alternativas 1.a y 1.b

Elementos	Cantidad	Precio Unitario USD	Precio total USD	
SWITCH PRINCIPAL				
Chasis con 3 backplanes independientes con capacidad para 8 módulos	1	5500	5500	
Fuente de poder principal	1	1900	1900	
Fuente de poder redundante	1	1500	1500	
Módulo de administración del procesador	1	10000	10000	
Módulo FDDI 100 Mbps de 2 puertos	6	7000	42000	
			SUBTOTAL	**60900**
SWITCH DE SERVIDORES				
Chasis con 1 backplane con capacidad para 5 módulos	1	4000	4000	
Fuente de poder principal	1	1900	1900	
Fuente de poder redundante	1	1500	1500	
Módulo de administración del procesador	1	10000	10000	
Uplink FDDI	1	3200	3200	
Módulo Fast Ethernet (10/20/100/200 Mbps autosensing) de 8 puertos de FO	2	6000	12000	
Módulo Token Ring (16 Mbps) de 8 puertos	1	4000	4000	
			SUBTOTAL	**36600**
SWITCHES SECUNDARIOS				
Chasis con 1 backplane con capacidad para 5 módulos	9	4000	36000	
Fuente de poder principal	9	1900	17100	
Fuente de poder redundante	9	1500	13500	
Módulo de administración del procesador	1	10000	10000	
Uplink FDDI	9	3200	28800	
a. Módulo Ethernet 10 Mbps de 24 puertos	31	7000	217000	
b. Módulo Fast Ethernet (10/20/100/200 Mbps autosensing) de 24 puertos	31	12000	372000	
			SUBTOTAL a.	**322400**
			SUBTOTAL b.	**477400**
INTERFACES DE RED				
Para servidores				
Fast Ethernet (100/200 Mbps)	12	150	1800	
Para estaciones				
a. Ethernet 10BaseT (4to y 6to pisos)	166	60	9960	
b. Fast Ethernet 100/200 Mbps (Todas las estaciones de trabajo)	741	100	74100	
			SUBTOTAL a.	**11760**
			SUBTOTAL b.	**75900**
				TOTAL 2.a **431660**
				TOTAL 2.b **650800**

Tabla 5.6 Costo de equipamiento de las alternativas 2.a y 2.b

Elementos	Cantidad	Precio Unitario USD	Precio total USD	
SWITCH PRINCIPAL				
Chasis con 3 backplanes independientes con capacidad para 8 módulos	1	5500	5500	
Fuente de poder principal	1	1900	1900	
Fuente de poder redundante	1	1500	1500	
Módulo de administración del procesador	1	10000	10000	
Módulo ATM 155 Mbps de 12 puertos para fibra multimodo	1	15000	15000	
			SUBTOTAL	**33900**
SWITCH DE SERVIDORES				
Chasis con 1 backplane con capacidad para 5 módulos	1	4000	4000	
Fuente de poder principal	1	1900	1900	
Fuente de poder redundante	1	1500	1500	
Módulo de administración del procesador	1	10000	10000	
(Uplink) Módulo ATM para 2 puertos y APIM ST	1	5000	5000	
Módulo Fast Ethernet (10/20/100/200 Mbps autosensing) de 8 puertos de FO	2	6000	12000	
Módulo Token Ring (16 Mbps) de 8 puertos	1	4000	4000	
			SUBTOTAL	**38400**
SWITCHES SECUNDARIOS				
Chasis con 1 backplane con capacidad para 5 módulos	9	4000	36000	
Fuente de poder principal	9	1900	17100	
Fuente de poder redundante	9	1500	13500	
Módulo de administración del procesador	1	10000	10000	
(Uplink) Módulo ATM para 2 puertos y APIM ST	9	5000	45000	
a. Módulo Ethernet 10 Mbps de 24 puertos	31	7000	217000	
b. Módulo Fast Ethernet (10/20/100/200 Mbps autosensing) de 24 puertos	31	12000	372000	
			SUBTOTAL a.	**338600**
			SUBTOTAL b.	**493600**
INTERFACES DE RED				
Para servidores				
Fast Ethernet (100/200 Mbps)	12	150	1800	
Para estaciones				
a. Ethernet 10BaseT (4to y 6to pisos)	166	60	9960	
b. Fast Ethernet 100/200 Mbps (Todas las estaciones de trabajo)	741	100	74100	
			SUBTOTAL a.	**11760**
			SUBTOTAL b.	**75900**
			TOTAL 3.a	**422660**
			TOTAL 3.b	**641800**

Tabla 5.7 Costo de equipamiento de las alternativas 3.a y 3.b

Elementos	Cantidad	Precio Unitario USD	Precio total USD	
SWITCH PRINCIPAL				
Chasis con 3 backplanes independientes con capacidad para 8 módulos	1	5500	5500	
Fuente de poder principal	1	1900	1900	
Fuente de poder redundante	1	1500	1500	
Módulo de administración del procesador	1	10000	10000	
Módulo Gigabit Ethernet de 2 puertos para FO	6	5600	33600	
			SUBTOTAL	**52500**
SWITCH DE SERVIDORES				
Chasis con 1 backplane con capacidad para 5 módulos	1	4000	4000	
Fuente de poder principal	1	1900	1900	
Fuente de poder redundante	1	1500	1500	
Módulo de administración del procesador	1	10000	10000	
Uplink Gigabit Ethernet	9	2800	25200	
Módulo Fast Ethernet (10/20/100/200 Mbps autosensing) de 8 puertos de FO	2	6000	12000	
Módulo Token Ring (16 Mbps) de 8 puertos	1	4000	4000	
			SUBTOTAL	**58600**
SWITCHES SECUNDARIOS				
Chasis con 1 backplane con capacidad para 5 módulos	9	4000	36000	
Fuente de poder principal	9	1900	17100	
Fuente de poder redundante	9	1500	13500	
Módulo de administración del procesador	1	10000	10000	
Uplink Gigabit Ethernet mas APIM ST	9	7500	67500	
a. Módulo Ethernet 10 Mbps de 24 puertos	31	7000	217000	
b. Módulo Fast Ethernet (10/20/100/200 Mbps autosensing) de 24 puertos	31	12000	372000	
			SUBTOTAL a.	**361100**
			SUBTOTAL b.	**516100**
INTERFACES DE RED				
Para servidores				
Fast Ethernet (100/200 Mbps)	12	150	1800	
Para estaciones				
a. Ethernet 10BaseT (4to y 6to pisos)	166	60	9960	
b. Fast Ethernet 100/200 Mbps (Todas las estaciones de trabajo)	741	100	74100	
			SUBTOTAL a.	**11760**
			SUBTOTAL b.	**75900**
			TOTAL 4.a	**483960**
			TOTAL 4.b	**703100**

Tabla 5.8 Costo de equipamiento de las alternativas 4.a y 4.b

Elementos	Cantidad	Precio Unitario USD	Precio total USD	
SWITCH PRINCIPAL				
Chasis con 3 backplanes independientes con capacidad para 8 módulos	1	5500	5500	
Fuente de poder principal	1	1900	1900	
Fuente de poder redundante	1	1500	1500	
Módulo de administración del procesador	1	10000	10000	
Módulo ATM 155 Mbps de 12 puertos para fibra multimodo	1	15000	15000	
			SUBTOTAL	**33900**
SWITCH DE SERVIDORES				
Chasis con 1 backplane con capacidad para 5 módulos	1	4000	4000	
Fuente de poder principal	1	1900	1900	
Fuente de poder redundante	1	1500	1500	
Módulo de administración del procesador	1	10000	10000	
(Uplink) Módulo ATM para 2 puertos y APIM ST	1	5000	5000	
Módulo ATM 25 Mbps de 8 puertos de fibra multimodo	2	5400	10800	
Módulo Token Ring (16 Mbps) de 8 puertos	1	4000	4000	
			SUBTOTAL	**37200**
SWITCHES SECUNDARIOS				
Chasis con 1 backplane con capacidad para 5 módulos	9	4000	36000	
Fuente de poder principal	9	1900	17100	
Fuente de poder redundante	9	1500	13500	
Módulo de administración del procesador	1	10000	10000	
(Uplink) Módulo ATM para 2 puertos y APIM ST	9	5000	45000	
a. Módulo Ethernet 10 Mbps de 24 puertos	31	7000	217000	
b. Módulo Fast Ethernet (10/20/100/200 Mbps autosensing) de 24 puertos	31	12000	372000	
c. Módulo ATM 25 Mbps de 24 puertos	31	16000	496000	
			SUBTOTAL a.	**338600**
			SUBTOTAL b.	**493600**
			SUBTOTAL c.	**617600**
INTERFACES DE RED				
Para servidores				
ATM de 25 Mbps	12	400	4800	
Para estaciones				
a. Ethernet 10BaseT (4to y 6to pisos)	166	60	9960	
b. Fast Ethernet 100/200 Mbps (Todas las estaciones de trabajo)	741	100	74100	
c. ATM (25 Mbps) todas las estaciones	741	250	185250	
			SUBTOTAL a.	**14760**
			SUBTOTAL b.	**78900**
			SUBTOTAL c.	**190050**
			TOTAL 5.a	**424460**
			TOTAL 5.b	**643600**
			TOTAL 5.c	**878750**

Tabla 5.9 Costo de equipamiento de las alternativas 5.a, 5.b y 5.c

Elementos	Cantidad	Precio Unitario USD	Precio total USD	
SWITCH PRINCIPAL				
Chasis con 3 backplanes independientes con capacidad para 8 modulos	1	5500	5500	
Fuente de poder principal	1	1900	1900	
Fuente de poder redundante	1	1500	1500	
Módulo de administración del procesador	1	10000	10000	
Módulo ATM 155 Mbps de 12 puertos para fibra multimodo	1	15000	15000	
			SUBTOTAL	**33900**
SWITCH DE SERVIDORES				
Chasis con 1 backplane con capacidad para 5 módulos	1	4000	4000	
Fuente de poder principal	1	1900	1900	
Fuente de poder redundante	1	1500	1500	
Módulo de administración del procesador	1	10000	10000	
(Uplink) Módulo ATM para 2 puertos y APIM ST	1	5000	5000	
Módulo ATM 155 Mbps de 8 puertos de fibra multimodo	2	12000	24000	
Módulo Token Ring (16 Mbps) de 8 puertos	1	4000	4000	
			SUBTOTAL	**50400**
SWITCHES SECUNDARIOS				
Chasis con 1 backplane con capacidad para 5 módulos	9	4000	36000	
Fuente de poder principal	9	1900	17100	
Fuente de poder redundante	9	1500	13500	
Módulo de administración del procesador	1	10000	10000	
(Uplink) Módulo ATM para 2 puertos y APIM ST	9	5000	45000	
a. Módulo Ethernet 10 Mbps de 24 puertos	31	7000	217000	
b. Módulo Fast Ethernet (10/20/100/200 Mbps autosensing) de 24 puertos	31	12000	372000	
c. Módulo ATM 25 Mbps de 24 puertos	31	16000	496000	
d. Módulo ATM 155 Mbps de 24 puertos	31	30000	930000	
			SUBTOTAL a.	**338600**
			SUBTOTAL b.	**493600**
			SUBTOTAL c.	**617600**
			SUBTOTAL d.	**1051600**
INTERFACES DE RED				
Para servidores				
ATM 155 Mbps FO	12	2000	24000	
Para estaciones				
a. Ethernet 10BaseT (4to y 6to pisos)	166	60	9960	
b. Fast Ethernet 100/200 Mbps (Todas las estaciones de trabajo)	741	100	74100	
c. ATM (25 Mbps) todas las estaciones	741	250	185250	
d. ATM (155 Mbps) todas las estaciones	741	1700	1259700	
			SUBTOTAL a.	**33960**
			SUBTOTAL b.	**98100**
			SUBTOTAL c.	**209250**
			SUBTOTAL d.	**1283700**

TOTAL 6.a	**456860**
TOTAL 6.b	**676000**
TOTAL 6.c	**911150**
TOTAL 6.d	**2419600**

Tabla 5.10 Costo de equipamiento de las alternativas 6.a, 6.b, 6.c y 6.d

Alternativa	Vida útil (t)	Costo de equipamiento USD / vida útil	Costo de desarrollo y operación/ vida útil	Beneficios tangibles / vida útil	Total beneficios / vida útil	Total costos / vida útil	Total (Beneficios menos costos) / vida útil	Tasa interés anual (r = 10%)	Factor $(1+r)^t$	Valor presente	Indice de valor presente repecto al máx
1.a	5	370410.00	21800.00	294607.50	294607.50	392210.00	-97602.50	0.10	1.61	-60604.00	-0.57
1.b	8	589550.00	29100.00	709292.00	709292.00	618650.00	90642.00	0.10	2.14	42285.00	0.40
2.a	5	431660.00	33300.00	294607.50	294607.50	464960.00	-170352.50	0.10	1.61	-105776.00	-1.00
2.b	10	650800.00	55500.00	886615.00	886615.00	706300.00	180315.00	0.10	2.59	69519.00	0.66
3.a	5	422660.00	33300.00	294607.50	294607.50	455960.00	-161352.50	0.10	1.61	-100188.00	-0.94
3.b	10	641800.00	55500.00	886615.00	886615.00	697300.00	189315.00	0.10	2.59	72989.00	0.69
4.a	5	483960.00	29800.00	294607.50	294607.50	513760.00	-219152.50	0.10	1.61	-136077.00	-1.28
4.b	12	703100.00	50300.00	1063938.00	1063938.00	753400.00	310538.00	0.10	3.14	98946.00	0.93
5.a	5	424460.00	25800.00	294607.50	294607.50	450260.00	-155652.50	0.10	1.61	-96648.00	-0.91
5.b	8	643600.00	42300.00	709292.00	709292.00	685900.00	23392.00	0.10	2.14	10912.00	0.10
5.c	6	878750.00	32400.00	626029.00	626029.00	911150.00	-285121.00	0.10	1.77	-160944.00	-1.52
6.a	5	456860.00	24300.00	294607.50	294607.50	481160.00	-186552.50	0.10	1.61	-115835.00	-1.09
6.b	12	676000.00	55100.00	1063938.00	1063938.00	731100.00	332838.00	0.10	3.14	106052.00	1.00
6.c	8	911150.00	38200.00	834705.33	834705.33	949350.00	-114644.67	0.10	2.14	-53483.00	-0.50
6.d	14	2419600.00	55600.00	2868621.00	2868621.00	2475200.00	393421.00	0.10	3.80	103600.00	0.98

Tabla 5.11 Cálculo del Valor Presente

5.6.1 ESTIMACIÓN DEL RIESGO ECONÓMICO

El riesgo económico es una medida de la probabilidad de que actualmente se obtengan los beneficios estimados. Las medidas del riesgo pueden darse en la siguiente escala:

1-3 Bajo riesgo (BR)
4-6 Mediano riesgo (MR)
7-10 Alto riesgo (AR)

5.6.2 ESTIMACIÓN DEL RIESGO OPERACIONAL

El riesgo operacional es una medida de la probabilidad del éxito que tenga la implementación y uso de los productos del sistema frente a los impedimentos que impone la estructura organizacional, políticas y ambiente operacional. La escala es igual a la del numeral 5.6.1.

5.6.3 ESTIMACIÓN DEL RIESGO TÉCNICO

El riesgo técnico es una medida de la probabilidad de que la tecnología trabaje apropiadamente. La escala es igual a la del numeral 5.6.1.

Las estimaciones sobre riesgos se detallan en la tabla 5.12. Nótese que mientras mayor sea el riesgo, el valor será más cercano a 10.

El cálculo del índice de riesgo mostrado en la tabla 5.12, es análogo al cálculo del índice del numeral anterior.

5.7 SELECCIÓN DE LA MEJOR ALTERNATIVA

Para la selección de la mejor alternativa debe observarse los resultados mostrados en la tabla 5.13.

La columna titulada "decisión", es el promedio de los índices correspondientes a beneficios y costos intangibles, valor presente y riesgo[55].

Considerando que los valores que se han ponderado en las tablas de evaluación han sido estimaciones, de acuerdo con la tabla 5.13, la toma de decisión final está entre las alternativas 4.b, 6.b y 6.d.

Debe observarse que el mejor puntaje lo tienen las alternativas 6.b y 6.d, pero un punto muy atenuante es la facilidad de migración que ofrece cada alternativa, pues esto reduce el valor de la inversión inicial requerida. En esto las mejores alternativas son las

[55] El valor de 1 para el índice de riesgo de una alternativa, indica que ella es la más riesgosa. Por esta razón en la tabla nos interesa calcular el valor del índice que menos riesgo tiene. Para esto, se resta de 1 el valor de índice de riesgo que se tenía inicialmente.

	Alternativas (puntaje entre 1 y 10)														
	1.a	*1.b*	*2.a*	*2.b*	*3.a*	*3.b*	*4.a*	*4.b*	*5.a*	*5.b*	*5.c*	*6.a*	*6.b*	*6.c*	*6.d*
Riesgos															
Riesgo económico															
Obsolecencia de equipo antes de terminar ciclo de vida útil	2	4	2	4	2	3	2	4	2	4	3	2	2	2	3
Inversión muy alta para espectativas de inversionistas	2	4	2	4	3	2	3	3	5	4	5	4	4	4	6
Riesgo operacional															
Dificultad de adaptación de técnicos a nueva tecnología	2	2	2	2	3	3	2	2	3	3	3	3	3	3	3
Inversión muy alta para espectativas de usuario final	3	2	3	2	3	2	3	2	4	3	3	3	2	2	2
Servicio y soporte con bajo tiempo de respuesta durante implementación	2	2	2	2	4	4	4	4	4	4	4	4	4	4	4
Riesgo técnico															
Sistema muy sensible	2	2	2	2	3	3	3	3	4	4	4	4	4	4	4
Servicio y soporte con bajo tiempo de respuesta en fase de producción	2	2	2	2	3	3	3	3	3	3	3	3	3	3	3
Posibilidad de que el subsistema de conectividad no funciene satisfactoriamente con aplicaciones esperadas	5	3	5	3	5	3	5	3	4	2	2	4	2	2	1
Enlentecimiento por uso interfaces de protocolos para garantizar compatibilidad (ej: LAN EMULATION, diferentes tamaños de trama)	2	2	4	4	4	4	2	2	5	5	2	4	4	2	2
Enlentecimiento por coliciones y cuellos de botella	3	2	3	2	3	2	3	2	3	2	2	3	2	2	2
Malfuncionamiento de redes virtuales	2	2	2	2	3	3	2	2	3	3	3	3	3	3	3
Riesgo promedio	*2.5*	*2.5*	*2.7*	*2.7*	*3.3*	*3*	*3*	*2.8*	*3.7*	*3.4*	*3.1*	*3.4*	*3*	*2.9*	*3*
Indice del riesgo respecto al máx.	0.68	0.68	0.73	0.73	0.89	0.81	0.81	0.76	1	0.92	0.84	0.92	0.81	0.78	0.81

Tabla 5.12 Análisis de riesgo

Alternativa	Vida útil	Ben. y cost. Intangibles sobre 10 (para el máx. beneficio)	Valor presente	Indice de valor presente repecto al máx	Riesgo promedio	Indice del riesgo respecto al máx.	1 - (Indice de riesgo)	DECISION	Inversión inicial	Con posibilidad de migración por partes
1.a	5	**7.4**	-60604.0	**-0.6**	2.5	**0.7**	0.3	**0.16**	370410.0	
1.b	8	**8.0**	42285.0	**0.4**	2.5	**0.7**	0.3	**0.51**	589550.0	
2.a	5	**7.2**	-105776.0	**-1.0**	2.7	**0.7**	0.3	**0.00**	431660.0	
2.b	10	**8.1**	69519.0	**0.7**	2.7	**0.7**	0.3	**0.58**	650800.0	
3.a	5	**7.4**	-100188.0	**-0.9**	3.3	**0.9**	0.1	**-0.03**	422660.0	
3.b	10	**8.4**	72989.0	**0.7**	3.0	**0.8**	0.2	**0.57**	641800.0	
4.a	5	**7.7**	-136077.0	**-1.3**	3.0	**0.8**	0.2	**-0.11**	483960.0	
4.b	12	8.5	98946.0	0.9	2.8	0.8	0.2			
5.a	5	**7.6**	-96648.0	**-0.9**	3.7	**1.0**	0.0	**-0.05**	424460.0	
5.b	8	**8.2**	10912.0	**0.1**	3.4	**0.9**	0.1	**0.33**	643600.0	
5.c	6	**8.1**	-160944.0	**-1.5**	3.1	**0.8**	0.2	**-0.18**	878750.0	
6.a	5	**7.8**	-115835.0	**-1.1**	3.4	**0.9**	0.1	**-0.08**	456860.0	
6.b	12	8.7	106052.0	1.0	3.0	0.8	0.2			
6.c	8	**8.5**	-53483.0	**-0.5**	2.9	**0.8**	0.2	**0.19**	911150.0	
6.d	14	9.1	103600.0	1.0	3.0	0.8	0.2			

Tabla 5.13 Resultados

4.b y 6.b. Esto puede observarse en la columna titulada "Con posibilidad de migración por partes" de la tabla 5.13, donde se muestra la inversión inicial requerida para las alternativas 4.b y 6.b, si se desearía considerar un proceso de migración por partes. La alternativa 6.d, no tiene la posibilidad de ser implementada por partes, pues su tecnología involucra un cambio total en la red desde el principio.

De los párrafos anteriores, y considerando que la alternativa 6.b provee facilidad de migración con una inversión inicial relativamente baja (manteniendo la tecnología actual en estaciones y migrando con el tiempo hacia 100BaseT), a diferencia de la alternativa 6.d que requiere una inversión inicial alta ineludible, se considera que la mejor alternativa para las necesidades que se han planteado es la alternativa 6.b.

Capítulo VI

Conclusiones y recomendaciones

VI. CONCLUSIONES Y RECOMENDACIONES

- La infraestructura de transporte y el subsistema de conectividad, son partes indispensables en una red de datos. Es sumamente importante dedicar el tiempo que sea necesario a su planificación y diseño antes de proceder a su implementación.
- Los modelos ayudan a que se realicen diseños "modulares", que permiten tener sistemas abiertos basados en estándares.
- Los sistemas abiertos basados en estándares, permiten la compatibilidad de productos entre múltiples proveedores.
- El modelo de referencia OSI es útil tanto a los diseñadores de redes como a sus administradores.
- Si bien el modelo de referencia OSI no coincide plenamente con todos los *stacks* de protocolos existentes, permite tener una visión clara del funcionamiento estratificado de cada uno de ellos.
- Las redes de datos están en permanente evolución, lo que determina que los técnicos que trabajan con ellas deban estar consecuentemente en permanente preparación.
- Un sistema estructurado es en resumen un sistema organizado, documentado, productivo, seguro, y fácil de administrar. Se recomienda la implementación de redes estructuradas de datos, aunque su costo inicial sea más alto que el de una red convencional.
- Se recomienda la homogeneidad y simetría de sistemas estructurados, con el objeto de facilitar su administración. Esto en la práctica, significa mejores tiempos de respuesta en atención de problemas.
- Un buen diseño de un sistema estructurado de datos permite mejorar tiempos de respuesta en atención a nuevos requerimientos y ahorro en costos de mantenimiento y remodelación.
- Actualmente debe considerarse el diseño íntegro de una red de telecomunicaciones, donde se incluyan servicios de voz, video y datos. El diseño de cada parte puede realizarse por separado, pero con miras a una integración global de telecomunicaciones. En esta tesis se ha realizado el análisis y diseño correspondiente a la parte de datos de una red LAN.
- El diseño de una red estructurada de datos incluye el diseño de cuatro partes: infraestructura de transporte, subsistema de conectividad, servidores y estaciones de trabajo. La presente tesis ha enfocado su estudio a las dos primeras. El análisis y diseño se ha realizado para el subsistema de conectividad, considerando una infraestructura planteada. Sin embargo, es recomendable que el diseño de estas dos partes sea realizado conjuntamente, determinando objetivos claros en cuanto a topologías, sistemas de administración, etc.
- Debido al crecimiento en capacidades de las redes WAN, y principalmente a las posibilidades de información que presenta, el diseño de redes LAN debe estar orientado a una total compatibilidad con tecnologías WAN existentes.
- Es importante tomar en cuenta la evolución que ha tenido la tecnología de comunicaciones y redes de datos, para poder estimar cual puede ser su futura tendencia. Es recomendable desarrollar ese "instinto", para que en función de un

conocimiento previo, se puedan realizar proyecciones al futuro, de tal forma que determinados eventos puedan ser anticipados.

- Se recomienda la utilización de tecnologías probadas y de amplia difusión a escala mundial, para garantizar en cierto modo la estabilidad de esa tecnología durante un período considerable.
- Se recomienda el uso de equipos, dispositivos y aditamentos fabricados por empresas que tenga su renombre y soporte a escala mundial. Debe tenerse cuidado en especial con los dispositivos del subsistema de conectividad, pues si bien se habla de sistemas abiertos, esto en la práctica no siempre se cumple. En la medida de lo posible, es recomendable la compra de equipos a un único fabricante, con el objeto de garantizar su total compatibilidad.
- Se considera que el *stack* de protocolos TCP/IP, actualmente es el más difundido a escala mundial, y por tanto el de mejores proyecciones a futuro. La razón de mayor peso es posiblemente su gran difusión en la gran red de INTERNET. Se recomienda por tanto, considerar la implementación del mencionado *stack*, como el único a utilizarse en redes de área local (tratando de conservar los criterios de homogeneidad y simetría planteados en esta tesis) con proyecciones de conexión a redes WAN.
- El tamaño de redes de comunicaciones, cada vez se vuelve más subjetivo. Esto se debe a la evolución tecnológica que se ha producido en la infraestraestructura de transporte y subsistemas de conectividad a escala mundial. Cada vez son más comunes los requerimientos de información que se hacen en línea, entre dos puntos ubicados en cualquier parte del mundo. El concepto de "*Intranet*" tiende a capturar los conceptos de redes LAN, MAN y WAN. Es decir, es menos preocupante la concepción de distancia, y se vuelve más importante el concepto de disponibilidad de información.
- El sistema de cableado estructurado, es una infraestructura de transporte estructurada actualmente en vigencia. En el futuro se esperan infraestructuras de transporte estructuradas sin cable.
- El subsistema de conectividad es más susceptible en cuanto a cambios y obsolescencia que la infraestructura de transporte. Por esta razón, durante la vida útil de una infraestructura de transporte, es posible que se tengan varios períodos con diferentes subsistemas de conectividad, cuyos reemplazos o actualizaciones se realizan por motivos de obsolescencia antes que por mal funcionamiento. Es recomendable que en el diseño teórico del subsistema de conectividad, el tiempo de vida útil estimado sea ponderado a una meta ideal, mientras que en la práctica debe tenerse en cuenta que la mayoría de tecnologías, especialmente en el subsistema de conectividad alcanzan su obsolescencia en períodos relativamente cortos (3, 4 ó 5 años).
- En general, es recomendable, que en cualquier análisis que se realice deba considerarse tanto la parte cualitativa como la cuantitativa. Sin embargo, en determinadas circunstancias en las que se requiera un criterio a priori y donde el riesgo en costo no sea significativo, bastará con un análisis cualitativo para implementar la solución.
- Una de las tendencias que actualmente está tomando fuerza, es la necesidad del manejo de tráfico tipo multimedia, por sus consecuentes ventajas en servicios y aplicaciones. Por esta razón, se recomienda considerar esta variable en el diseño e implementación de nuevas redes.

- Cuando se realiza la modificación o actualización de una red existente y en servicio, es sumamente importante se realice un proceso de migración detallado, para evitar problemas en la red que está en funcionamiento. Adicionalmente, debe considerarse la posibilidad de reutilizar la tecnología que está siendo ocupada, en incluirla dentro del nuevo diseño, con el fin de prolongar su tiempo de vida útil.

Bibliografía

BIBLIOGRAFIA

3COM "Transcend-Integrated Management for Data Networks", 3Com Strategic Directions, August 1993

3COM: "100BASE-T Fast Ethernet", 3Com Strategic Directions, October 1994

3COM: "3TECH -Switches and Routers Technical Paper", Internet, October 3, 1996

3COM: "3TECH -The BRASICA Chip Set Architecture", Vol , Number 1, Internet, Jan 1996

3COM: "3TECH The 3COM technical Journal", Vol 5 Number 1, January 1994

3COM: "3TECH The 3COM technical Journal", Vol 5 Number 4, October 1994

3COM: "3TECH The 3COM technical Journal", Vol 6 Number 2, April 1995

3COM: "Boundary Routing System Architecture", 3Com Strategic Directions, August 1993

3COM: "Guía para adaptadores de red 3com", Febrero 1994

3COM: "Guide to 3Com Hubs", September 1994

3COM: "Guide to 3Com Internetworking Products", July 1994

3COM: "High-Performance Scalable Networking with Routed ATM", 3Com Strategic Directions, April 1994

ALCATEL Cabling System: "Cabling Vision", International Newsletter, April 1996

ALCATEL Cabling System: "Component Catalogue", Brussel-Belgium, January 1996

ALCATEL Cabling System: "Concept Manual", Ver 2.0, 1996

ALCATEL Cabling System: "Connecting to the future", Brussel-Belgium, January 1996

American Research Group, "Bridges, Routers & Switches", Rev 6.0, June 1996

American Research Group, "Networking Protocol Fundamentals", Rev 5.0A, 1996

ANSI/EIA/TIA: "Commercial Building Standard for Telecommunications Pathways and Spaces", ANSI/EIA/TIA-569, October 15 1990

ANSI/EIA/TIA: "Commercial Building Telecommunications Cabling Standard", ANSI/EIA/TIA-568-A, October 1995

Bay Networks: "BayStack 10BASE-T Stackable Hubs", Anixter, Internet, 1996

Cisco Systems: "CiscoPro EtherSwitch 1400 User Guide", 1996

Cisco Systems: "FDDI Internetworking", Technology Brief, April 1994

Cisco Systems: "Introduction to Cisco Router", Course Introduction, USA, 1996

Computer and Communication: "Standards and Cross References", Internet 1997

Data Communications, "Classical IP Over ATM: Astatus Report", Tech Tutorials, Internet, December 1995

ERICSSON Cabling System: "Cableado Integral Estructurado", 1993

ERICSSON Cabling System: "Designing a transport Infraestructure", 1994

Hewlett-Packard Company: "Ethernet Switching", Internet, May 1996

Hidalgo Pablo Ing., "Teoría de Comunicación Digital", Material de estudio Politécnica Nacional, 1994

IBM: "IBM 8271 Nways Ethenet LAN Switch", Publication 1994

IBM: "IBM 8272 Nways Token-ring LAN Switch", Publication 1994

IBM: "IBM 8285 Nways ATM Workgroup Switch", Publication 1994

IBM: "Introducción a Internetworking", Seminario Internacional de Internetworking, Perú, 1995

IOL: "Network Management RFCs", Internet, 1997

Ledesma Bolívar Ing., "Estudio del sistema de cableado estructurado para el Banco Central del Ecuador", Quito, 1996

Marco Jarrín Ing.: "Redes de datos basados en la conmutación de paquetes", 1997

MOD-TAP: "Wordwide applications & components", 1995-1996

Novell Education: "Netware TCP/IP Transport", Revisión 1.01, 1995

Novell Education: "Tecnologías de conectividad", Revisión 1.01, 1995

Pras Aiko: "Network Management Architectures", CTIT Ph. D-thesis series No 95-02, Netherlands, 1995

SERIX : "Network Cards", Internet, Feb 1997

Stevenson Douglas, "Network Management White Paper", Buffalo University, Internet, Apr 1995

SVEC Computer Corporation: "Network Interface Cards", Internet, Feb 1997

Tanenbaum, A.S.:"Computer Networks". Prentice-Hall, 1988

Thompson Peter: " Routing & Router Architecture", Internet, Jan 1995

TIA/EIA: "Additional Horizontal Cabling Practices for Open Offices", TSB-75, Draft 16, June 6, 1996

Transport Management Group, "TIA/EIA 606 - Administration Standard for the Telecommunications Infrastructure of Commercial Buildings", Internet, 1997

ANEXO A.

Polarización y Secuencia

Polarización.- Está definido como el factor de forma físico de una interfaz de enchufe modular o roseta. Si la polarización del equipo no empareja con la interfaz del cable construido, un adaptador mecánico debería ser usado para conversión. El conector macho se lo conoce como *plug*, y el conector hembra como *jack*.

Opciones de polarización.

WE4W/WE6W. Se lo conoce generalmente como "RJ11" y "RJ12". Este era el estándar especificado de polarización modular como estándar de voz por las compañías de teléfonos de los Estados Unidos.

Las siglas WE representan Western Electric, el número 4 ó 6 indica el número de alambres, W es de wire (alambre). Así, WE4W es una interfaz de 4 alambres.

Los pines son numerados del 1al 6 para WE6W, y del 2 al 5 para WE4W.

WE8W. Generalmente conocido como "RJ45". Puede contener 8 hilos y sus pines son numerados del 1 al 8. Por su tamaño no puede encajar en un enchufe RJ11 o RJ12, sin embargo un conector RJ11 o RJ12 si puede encajar dentro de un enchufe RJ45.

WE8K. Generalmente conocidos como "RJ45 Keyed", fueron desarrollados como una alternativa de polarización para líneas de teléfono especializadas (balanceadas). Idénticas a RJ45 pero con la adición de un "diente" a uno de sus lados.

Debe notarse que el enchufe WE8W no puede aceptar al conector WE8K, sin embargo al contrario sí.

MMJ. (Modified Modular Jack) Esta polarización fue desarrollada por Digital Equipment Corporation (DEC) para crear un enchufe de datos que no es interconectable con ninguno de los otros interfaces. Consiste de un factor de forma de un WE6W con un diente de seguro en el lado derecho. El conector MMP (Modified Modular Plug) solamente empata con un enchufe MMJ.

Secuencia.- Está definida como el orden en el cual la integración de los pares es terminada dentro de los pines de la interfaz modular, es decir, cuales pines son el par número 1. Cada par está designado como un conductor "Tip" y un conductor "Ring". El par número 1 estará designado como "T1" y " R1". La secuencia es extremadamente importante, ya que un error puede resultar en altos niveles de ruido y crosstalk entre señales de pares mal secuenciados. Algunas secuencias son aplicables solamente a ciertas polarizaciones.

Opciones de secuencia.

EIA 568A. Es la más nueva de las opciones de secuencias publicadas en el EIA *Commercial Building Cabling Specification Draft 9.0* como la opción de secuencia preferida para la terminación del cable de datos UTP (este es el estándar internacional ISDN). Es similar a la secuencia 568B excepto que tienen transpuestos los pares #2 y #3. Esto provee compatibilidad hacia atrás a la secuencia USOC para dos pares al contrario del par único de 568B.

EIA 568B. Comenzó como la opción de secuencia más difundida para las instalaciones de datos. Es también un subgrupo especificado por la IEEE 802.3 10BASE-T Ethernet sobre el estándar de par trenzado. Esta secuencia es solamente aplicable a las polarizaciones de 8 hilos (WE8W y WE8K).

En la secuencia 568B, el par #1 y el par #3 corresponden al par #1 y par #2 de la secuencia USOC, proveyendo compatibilidad hacia atrás con sistemas de dos pares (tales como voz analógica).

USOC. Históricamente es la opción de secuencia más utilizada por los sistemas de teléfonos de los Estados Unidos. Los pares son "anidados": el par 1 en el centro, el par 2 luego, etc. Esto mantiene la continuidad par a par cuando, por ejemplo, un equipo de un par es conectado a un circuito de 4 pares.

USOC es aplicable a polarizaciones WE2W, WE4W, WE6W, WE8W, y WE8K.

356A. Es una versión de 3 pares de 568B, dejando el par 4 desconectado.

10BASE-T. Es usado con polarización WE8W/8K. Esta es una modificación de la secuencia 568B, dejando los pares 1 y 4 desconectados. Esto provee un nivel adicional de protección de la interconexión entre equipo de voz y datos, pues los datos ocupan los pines 4 y 5 que para esta secuencia, no tienen conexión.

Open DECconnect. Es una variación de 3 pares de la secuencia EIA 568A dejando el par 1 desconectado (pines 4 y 5 están abiertos).

DEC. Esta secuencia fue desarrollada por Digital Equipment Corporation para usao en su sistema de cableado estructurado original DECconnect de UTP para soportar RS423 con compatibilidad hacia atrás con RS232.

ANEXO B.

"Resumen de elementos y documentación de un sistema de cableado estructurado según el estándar ANSI/EIA/TIA-606 para la administración de redes estructuradas".

ELEMENTOS

A. Tabla de los elementos de la infraestructura

	RECORD	REQUIRED INFORMATION	REQUIRED LINKAGES
PATHWAYS AND SPACES	PATHWAY	Identifier Type Fill Loading	Cable Records Space Records Pathway Records Grounding Records
	SPACE	Identifier Type	Pathway Records Cable Records Grounding Records
WIRING	CABLE	Identifier Type Unterm. Pair/Cond. Nos. Damaged Pair/Cond. Nos. Available Pair/Cond. Nos.	Term. Position Records Splice Records Pathway Records Grounding Records
	TERMINATION HARDWARE	Identifier Type Damaged Position Numbers	Term. Position Records Space Records Grounding Records
	TERMINATION POSITION	Identifier Type User Code Cable Pair/Cond. Numbers	Cable Records Other Term. Pos. Records Term. Hardware Records Space Records
	SPLICE	Identifier Type	Cable Records Space Records
GROUNDING AND BONDING	TMGB	Identifier Busbar Type Grounding Cond. Identifier Resistance to Earth Date Measurement Taken	Bonding Cond. Records Space Records
	BONDING CONDUCTOR	Identifier Type Busbar Identifier	Grounding Busbar Records Pathway Records
	TGB	Identifier Type	Bonding Cond. Records Space Records

Tabla B.1 Información a registrarse en los elementos de un sistema de cableado estructurado

B. Diagrama de los elementos de la infraestructura

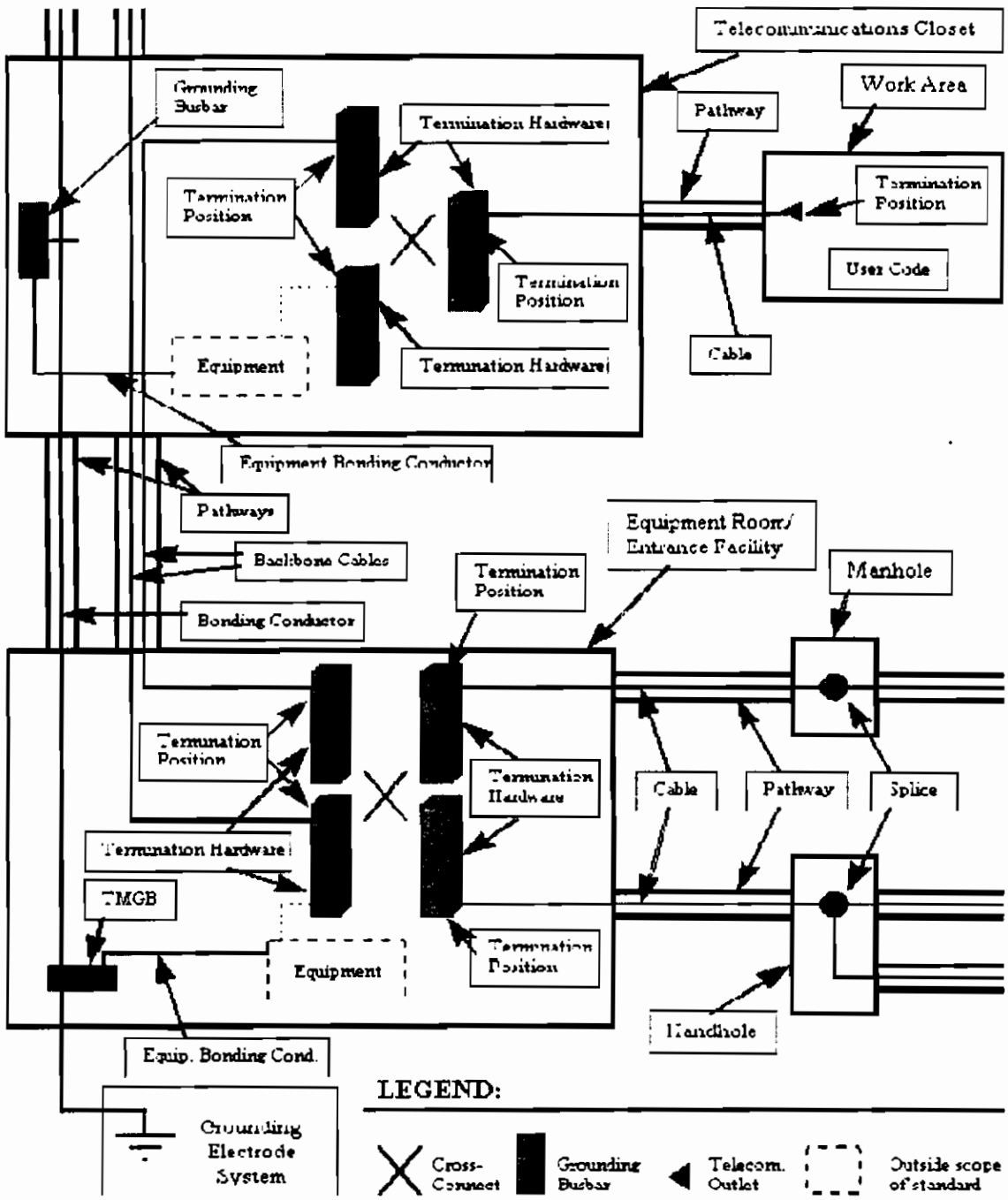


Figura B.1 Diagrama de los elementos de un sistema de cableado estructurado

C. Canaletas y espacios (*Pathways* and spaces)

Cada ***canalización-pathway*** (conduit, bandeja, canaleta amplia-raceway, etc) que lleva el medio de telecomunicaciones de espacio a espacio, debe tener un único identificador y etiqueta en cada punto terminal.

Los puntos intermedios donde 3 o más canaletas se unen deben ser etiquetados en su punto final.

Las canaletas (*pathways*) particionadas tales como un banco de ductos o conduit con un ducto interior deben tener identificadores únicos para cada partición.

Una canalización completa que une 2 ó más canaletas de diferentes tipos o tamaños, debe tratarse como una canalización separada a cada segmento.

Los sistemas particionados tales como pisos celulares, los cuales no son prácticos de etiquetar, deben ser documentados o dibujados.

Cada re*cord* de canalización debe incluir su tipo, su porcentaje actual de utilización (cuan lleno está actualmente), y su carga actual (peso por unidad de área) si es aplicable.

Cada identificador de canalización debe ser enlazado con los cables dentro de él, los espacios de telecomunicaciones en cada extremo, cualquier espacio de acceso a lo largo de su longitud, cualquier conexión a otra canalización, y el método de conexión a tierra.

Cada ***espacio de telecomunicaciones*** (cuarto de equipos, *closet* de telecomunicaciones, área de trabajo, facilidad de entrada, manhole, y handhole) deben ser individualmente identificados y etiquetados.

El identificador y el tipo de espacios debe ser grabado en re*cords*, y el identificador debe ser *enlazado (eslabonado)* a los ***pathways***, cables, y buses de conexión a tierra que terminan en ese espacio.

D. Cable

Cada cable debe ser identificado y etiquetado individualmente en cada extremo. Se recomienda la etiquetación en localizaciones intermedias.

Los cables empalmados del mismo tipo y número son administrados como un único cable, mientras que los cables empalmados de diferentes tipos o número de pares deben ser administrados separadamente.

Es recomendable que los componentes individuales de un cable híbrido (con diferentes tipos de subcomponentes) sean nombrados y etiquetados separadamente.

Cada re*cord* de cable debe indicar el tipo de cable por fabricante y diseño de fabricante, y debe documentar cada par/conductor en el cable.

Los pares de cables disponibles, dañados, o indeterminados deben ser señalados.

El identificador de cable debe ser enlazado (eslabonado) a todos las canaletas por las cuales pasa, a cualquier información de empalme, y al re*cord* de conexión a tierra.

Los conductores/pares individuales deben ser enlazados (eslabonados) a un ré*cord* de posición de terminación a cada extremo.

Cada pieza de hardware de terminación tal como un *patch panel* o bloque IDC, debe ser nombrado y etiquetado individualmente.

El tipo de hardware y cualquier posición de daño deben ser indicados.

Cada pieza de hardware de terminación debe ser enlazada (eslabonado) a un espacio de telecomunicaciones, a un ré*cord* de conexión a tierra, y a los ré*cords* de posición de terminación individual donde sea aplicable.

E. Empalmes (Splices)

Cada unión o empalme debe ser nombrada y etiquetada, y su tipo y espacio deben ser identificados y grabados en un ré*cord*. Un empalme en un cable administrado como un único cable debe ser nombrado y enlazado al identificador del cable.

Un identificador de empalme separado (con su tipo y espacio indicado) debe ser creado por cada empalme entre 2 cables cualquiera. Si el cable A es unido al cable B y C, entonces identificadores separados son requeridos para cada empalme entre los cables A y B y para el empalme entre los cables A y C.

El identificador de unión o empalme debe ser usado como la posición de terminación para cada par/conductor en el cable.

F. TMGB (Telecommunications Main Grounding Busbar)

El TGMB para cada edificio debe ser etiquetado como "TGMB" y debe tener un único identificador.

El re*cord* del TGMB debe incluir el identificador TGMB, tipo de busbar, el identificador del conductor de conexión a tierra (entre el TGMB y la tierra del edificio), la resistencia medida a la tierra (en ohms), y la fecha de la medición.

El identificador TGMB debe ser enlazado a los re*cords* del conductor de conexión a tierra (bonding conductor) y a los identificadores de espacio.

G. Conductores de conexión a tierra (Bonding Condutors)

Cada conductor de conexión a tierra del *backbone* (entre el TMGB y el TGB en cada uno de los *closets* de cableado) debe ser nombrado y etiquetado individualmente en cada extremo.

El conductor entre el TMGB y la tierra del edificio debe tener un único identificador y llevar una etiqueta de precaución para notificar al administrador de telecomunicaciones si el conductor es desconectado o removido.

Cada re*cord* del conductor de conexión a tierra debe incluir el identificador del conductor, el tipo de conductor y el identificador TMGB. Aquel debe ser enlazado a cada re*cord* del TGB y a los re*cords* de canaletas por donde pase.

Las canaletas del conductor de conexión a tierra son administradas de la misma forma en que se hace con las canaletas de cable normal.

Se recomienda que cualquier conductor de conexión a tierra desde el TGB al equipo local sean nombrados y etiquetados individualmente en su parte próxima al TGB.

H. TGB (Telecommunications Grounding Busbar)

Cada TGB debe ser nombrado y etiquetado individualmente.

El identificador del TGB debe empezar con el prefijo "TGB".

Cada re*cord* del TGB debe incluir el identificador del TGB y el tipo de TGB, y debe ser enlazado (eslabonado) a cada uno de los re*cords* de los conductores de conexión a tierra (bonding conductors) y a un identificador de espacio.

DOCUMENTACIÓN

El esquema de administración definido por el estándar ANSI/EIA/TIA-606 básicamente envuelve aspectos de documentación tales como etiquetas, records, dibujos, reportes, y órdenes de trabajo.

A. Tabla de los elementos de la infraestructura

Ver tabla B.1.

B. Dibujos

El re*cord* de los dibujos debe ser mantenido y debe contener el nombre, localización y tamaño de cada *pathway* y espacio.

Los re*cords* de los dibujos también indican la localización e identificador de todos las terminaciones de cable y cables de *backbone*. Se recomienda la indicación de la ruta del cable y las localizaciones de las uniones.

Los dibujos del plan de piso deben mostrar la localización e identificador de todas las salidas de telecomunicaciones.

El re*cord* de los dibujos para la infraestructura de conexión a tierra debe mostrar la localización del electrodo de tierra, la ruta del conductor de conexión a tierra desde el electrodo hasta el TMGB, y las localizaciones e identificadores de todos los busbar de conexión a tierra (TGB). Se recomienda la indicación de todas las rutas de los conductores bonding.

Para la mayoría de los dibujos mencionados, el estándar recomienda información adicional la cual podría ser de beneficio para el administrador.

C. Reportes

El estándar recomienda los siguientes reportes:

Reporte resumido de canalización el cual lista todas las canaletas por identificador e incluye sus tipos, porcentaje de llenado actual, y carga actual.

Reporte del contenido de canalización el cual lista todos los cables por identificador dentro de cada canalización.

Reporte resumido de espacio el cual lista todos los espacios por identificador e incluye sus tipos y localización.

Reporte resumido de cables el cual lista todos los cables por identificador e incluye sus tipos e identificadores de hardware de terminación para cada extremo.

- *Reporte resumido de conexión a tierra (Grounding/Bonding)* el cual lista cada TMGB y TGB por identificador e incluye sus tipos e identificadores del conductor de conexión a tierra.

Reporte del circuito extremo a extremo (en to end) el cual traza la conectividad de extremo a extremo. Este reporte lista cada circuito por código de ususario, identificador de cable, y posiciones de terminación.

Reporte de conexión de cruce para cada espacio el cual lista cada *cross-connect* por posición de terminación en ese espacio.

D. Ordenes de trabajo

Las órdenes de trabajo deben ser mantenidas y guardadas en archivos para cualquier tipo de modificación, adición o reparación a todos los elementos de la infraestructura los cuales son cubiertos por este estándar. Una orden de trabajo podría envolver espacios, canaletas, cables, uniones, terminaciones, o elementos de conexión a tierra sea individualmente o en combinaciones.

Cada elemento afectado por una orden de trabajo debe ser indicado en la orden de trabajo por su identificador y tipo.

Los ré*cords* afectados por la orden de trabajo deben ser actualizados.

El estándar recomienda que cada orden de trabajo indique el personal responsable de ejecutar los cambios físicos y la actualización del sistema de administración cuando se complete.